

Rapid Mission Assurance Assessment via Sociotechnical Modeling and Simulation

Michael Jay Lanham

CMU-ISR-15-104
May 2015

School of Computer Science
Institute of Software Research
Carnegie Mellon University
Pittsburgh, PA

Thesis Committee

Kathleen M. Carley (Chair)

Virgil D. Gligor

Jürgen Pfeffer

Robert Elder (George Mason University)

John Graham (United States Military Academy)

Submitted in partial fulfillment of the requirements
for the Degree of Doctor of Philosophy

Copyright © Michael J. Lanham

This work was supported in part by the Office of Naval Research MURI N000140811186, a joint grant from the National Security Agency and Army Research Office (ARO) under grants W911NF1310154, the Center for Computational Analysis of Social and Organizational Systems (CASOS), and the United States Military Academy. The views and conclusions contained in this document are those of the author and should not be interpreted as representing the official policies, either expressed or implied, of the Office of Naval Research, the National Security Agency, the Army Research Office, the US Army, or the U.S. Government.

Report Documentation Page				Form Approved OMB No. 0704-0188		
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.						
1. REPORT DATE 31 MAY 2015		2. REPORT TYPE Final		3. DATES COVERED		
4. TITLE AND SUBTITLE Rapid Mission Assurance Assessment via Sociotechnical Modeling and Simulation				5a. CONTRACT NUMBER MURI N000140811186		
				5b. GRANT NUMBER		
				5c. PROGRAM ELEMENT NUMBER		
6. AUTHOR(S) Lanham /Michael J.				5d. PROJECT NUMBER		
				5e. TASK NUMBER		
				5f. WORK UNIT NUMBER		
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) CASOS, Institute of Software Research, School of Computer Science, Carnegie Mellon University				8. PERFORMING ORGANIZATION REPORT NUMBER CMU-ISR-15-104		
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)		
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)		
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release, distribution unlimited.						
13. SUPPLEMENTARY NOTES The original document contains color images.						
14. ABSTRACT How do organizations rapidly assess command-level effects of cyber attacks? Leaders need a way of assuring themselves that their organization, people, and information technology can continue their missions in a contested cyber environment. To do this, leaders should: 1) require assessments be more than analogical, anecdotal or simplistic snapshots in time; 2) demand the ability to rapidly model their organizations; 3) identify their organization's structural vulnerabilities; and 4) have the ability to forecast mission assurance scenarios. Using text mining to build agent based dynamic network models of information processing organizations, I examine impacts of contested cyber environments on three common focus areas of information assurance—confidentiality, integrity, and availability. I find that assessing impacts of cyber attacks is a nuanced affair dependent on the nature of the attack, the nature of the organization and its missions, and the nature of the measurements. For well-manned information processing organizations, many attacks are in the nuisance range and that only multipronged or severe attacks cause meaningful failure. I also find that such organizations can design for resiliency and provide guidelines in how to do so.						
15. SUBJECT TERMS						
16. SECURITY CLASSIFICATION OF:				17. LIMITATION OF ABSTRACT UU	18. NUMBER OF PAGES 375	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified				

Keywords: Mission Assurance, Resilience, Assessment, Cyberspace Operations, Cyber, Organization Resilience, Rapid Modeling, Agent Based Model, ABM, Simulation, Modeling and Simulation

Dedicated to my wife, my children, and my country

Acknowledgements

It has been my great fortune to work with and for an outstanding dissertation committee in Kathleen M. Carley, Virgil D. Gligor, Jürgen Pfeffer, Robert Elder (Lieutenant General, US Air Force, Retired) and John Graham (Colonel, US Army). I am particularly indebted to Kathleen for her willingness to take on yet another Army officer, constrained to a very challenging Army time line. I have insufficient words or eloquence to thank everyone adequately, as I know my wife, my children, my family and my friends have missed me these last years.

Throughout this latest journey and on the paths to it, so many people have helped me in more ways than I can enumerate. I have been incredibly fortunate to have so many good people touch my life! Nevertheless, I offer my thanks to the supporting staff, administrators, and developers in the Center for Computational Analysis of Social and Organizational Systems ([CASOS](#)). I also offer special thanks to Geoffrey P. Morgan for all the many hours of brain storming, selfless assistance, rapid prototyping, tool development, conducting analysis, and being a friend! Many thanks also to Kenneth ‘Kenny’ Joseph for the hours he spent in developing, configuring, and debugging Construct, and helping me do the same. To Peter Landwehr, Wei Wei, and my other fellow doctoral seeking peers in CASOS, I offer my thanks!

The support I have received from the leadership and faculty at the United States Military Academy ([USMA](#)). Department of Electrical Engineering and Computer Science ([D/EECS](#)) has also been superb. The energy and effort they have contributed to me finishing this trek continues to humble me and generate my gratitude. From covering teaching and grading duties, simple words of encouragement, and forcing me to simply close my door to get work done, my friends and colleagues have been extremely helpful. Thank you also to Dr. Chris Okasaki, for his particular gift to me in being a volunteer editor of this written work. All errors in this text are despite his efforts at helping me be a clearer writer.

Abstract

How do organizations rapidly assess command-level effects of cyber attacks? Leaders need a way of assuring themselves that their organization, people, and information technology can continue their missions in a contested cyber environment. To do this, leaders should: 1) require assessments be more than analogical, anecdotal or simplistic snapshots in time; 2) demand the ability to rapidly model their organizations; 3) identify their organization's structural vulnerabilities; and 4) have the ability to forecast mission assurance scenarios. Using text mining to build agent based dynamic network models of information processing organizations, I examine impacts of contested cyber environments on three common focus areas of information assurance—confidentiality, integrity, and availability. I find that assessing impacts of cyber attacks is a nuanced affair dependent on the nature of the attack, the nature of the organization and its missions, and the nature of the measurements. For well-manned information processing organizations, many attacks are in the nuisance range and that only multipronged or severe attacks cause meaningful failure. I also find that such organizations can design for resiliency and provide guidelines in how to do so.

Table of Contents

Acknowledgements	v
Abstract	vii
Introduction	1
Thesis Statement	1
Scope	3
Definitions	4
Why is this important?	8
What will this dissertation do?	10
Literature Review	11
Introduction	11
Related Areas of Research	16
Related literature corpus and assessment	32
Conclusions	67
Data and Models	70
Introduction	70
Organization—a working definition	71
Organizations’ Self-Documentation	72
The Data to Model Process—an Overview	73
Two D2M generated DoD organizational models	77
Changes to empirical models in support of Agent Based Modeling	115
Conclusions	116
Network Analytics and Resilience	118
Resilience in what context?	119
Static resilience indicators	121
Metanetwork resilience indicators	122
New and adjusted metanetwork resilience indicators	123
Resilience indicators for strategic and operational models	132
Entropic and Targeted Attacks	150
Conclusions	166
Agent Based Models and Modeling	169
Agent based models and sociotechnical systems	170
Agent based models and cyber security research	171
Overview of Construct	172
Augmentation of D2M generated models	175
Experimental Design Setup	191
Conclusion	197
Simulations	198
Changes to Construct	198
Analysis	203
Omitting New Resilience Metric	203
Mitigations	212
Heuristics	217
Limitations and Future Work	223
Text-mining as basis of organizational modeling	223

Limitations of doctrine and written products as the basis of models.....	223
Cyber effects vs. methods-of-attack	225
Modeling and Simulations	225
Contributions.....	231
Insights and Surprises	233
References.....	237
Appendix 1 Definitions.....	1-1
Central Definitions.....	1-1
Alphabetical Definitions	1-7
Appendix 2 Literature Review Bibliometrics	2-1
Introduction.....	2-1
Process	2-1
Searches and Search Results.....	2-1
Pre-processing Collected Data.....	2-3
Importing Collected Data into ORATM	2-3
Import Node Sets and Networks	2-4
Cleaned Article node set	2-10
Cleaned Author node set.....	2-10
Cleaned Concept node set.....	2-10
Manipulate Networks.....	2-10
Appendix 3 Data to Model Implementation Details	3-1
Introduction.....	3-1
Retrieving input corpus.....	3-1
Corpus augmentation	3-5
Retrieving input corpus.....	3-6
Pre-processing DoD corpus	3-6
Metanetwork encoding heuristics for thesaurus refinement	3-8
Using frequency as culling decision input variable	3-11
Appendix 4 Virtual Experiment How-To Guide	4-1
SVN or other Shared-work Repository.....	4-1
Create a Directory Structure	4-1
Input Files	4-3
Updating Executables sent to the Condor cluster	4-7
Perl on submitting machine	4-8
Directories for Condor Virtual Experiment	4-9
Submitting to Condor for the Virtual Experiment	4-9
Post-Processing Outputs of Condor from a Virtual Experiment	4-10
Using R for Graph Generation.....	4-14
Appendix 5 Construct Input Files	5-15
Parameters files.....	5-15
Experimental Configuration File (Box-Behnken implementation)	16
Appendix 6 Construct input deck for operational and strategic simulation.....	6-1
Appendix 7 Additional Model Analysis, Tables, and Figures.....	7-1
Descriptive Statistics of Operational Model, Attacks, and Mitigations.....	7-1
Appendix 8 Lists of Tables, Figures, Equations and Acronyms.....	8-1
List of Tables	8-1

List of Figures	8-2
List of Equations	8-6
Acronyms	8-8
Appendix 9 Index.....	9-12

Introduction

How do organizations assess command-level effects of cyber attacks? Leaders need a way of assuring themselves that their organization, people, and information technology ([IT](#)) can continue the organizational missions in a contested cyber environment. To do this, leaders should: 1) require assessments be more than analogical, anecdotal or simplistic snapshots in time; 2) demand the ability to rapidly model their organizations; 3) identify their organization's structural vulnerabilities; and 4) have the ability to forecast mission assurance scenarios.

Of course, the nature of organizational dependence on IT varies, and assessments and forecasting of resilience to contested cyber environments should be nuanced to maintain credibility. This dissertation provides a repeatable methodology to conduct nuanced assessments of certain types of organizations, advances research of organizational resilience, and helps bridge gaps between related communities of interest and researchers.

Thesis Statement

Organizations can design themselves to improve their organizational resilience in contested cyber environments. They can do this by deliberately adjusting their formal and informal structures (human and [IT](#)) to reduce their susceptibility to events in contested cyber environments. They can also assess the improvements in resilience to contested cyber environments due to the chosen structural and functional mitigations and fold the assessed shortfalls into a continuous improvement cycle. The fundamental expectation is that organizations can indeed design their structures and their functions to be resilient to contested cyber environments. Consequences of such efforts include organizations projecting and achieving higher levels of mission assurance than they might otherwise.

Using a rapid data to modeling approach, this research shows that organizations can develop complex network-based models of themselves and their characteristics that impact the ability of the organization to continue its mission(s). These models are multimodal in that there are multiple node types and multiplex in that there can be multiple links between nodes of the same types as well as links between nodes of different types. Node types include people, IT systems, resources, IT resource, tasks, knowledge, roles, and beliefs. The models

are compatible with analysis techniques from graph theory and social network analysis ([SNA](#)) research. The models also support over time analysis, also called dynamic network analysis ([DNA](#)). These analytic techniques support objective analysis across multiple dimensions as well as various levels of aggregation or disaggregation of nodes and links. The rapidity and flexibility of these network-based models lend themselves to rapid self-assessments, especially when compared to more traditional cyber and general-purpose risk assessment frameworks' data gathering and analysis techniques.

This research and dissertation shows it is feasible and appropriate to convert these multidimensional models to inputs for multiagent simulation environments. The outputs of the simulations support assessments of organizations in nominal and degraded cyber environments. Simulating effects of contested cyber environments (i.e., loss of confidentiality, loss of integrity, and loss of availability), the work shows that structural mitigations (i.e., modifications of the quantity and frequency of human-to-human links) as well as modifications to various IT dependencies (i.e., modifications of the quantity of IT systems and rapidity of replacements being brought into the system) are feasible and somewhat effective at reducing the impacts of contested cyber environments. It helps establish that modeling and simulation (M&S) can forecast the efficacy of mitigations before leaders commit real and potentially scares resources. With efficacious mitigations, organizations and leaders can increase their confidence of mission assurance in contested cyber environments.

The research and dissertation also reveal that granularity of distinctions are essential in discussing the types of organizations put under test, as well as interpreting the results of virtual experiments. The military organizations modeled in this work generalize to some types of organizations, but certainly not all, and certainly not to IT dominated organizations (e.g., exchange traded funds ([ETF](#))), or manufacturing lines. I also choose to limit the research to small sub-sets of the organization, with the expectation that sub-groups may suffer different effects, again requiring nuance in group identification and effects. One result of this research, explored further in the related work portion, is there is substantial room for increased cooperation between research communities in organizational behavior and resilience, organizational design, and cyberspace operations and security.

Scope

There are multitudes of ways to scope a dissertation in this research area. The following, combined with the definitions in [Definitions](#) (starting on page [1-1](#)), delineate the boundaries of the problem space for both practical and tractability reasons.

The analyses for the various organizations under test focus on the formal decision makers of the organization—that is they are command-level analyses. However, decision makers do not operate in a vacuum; they have surrounding and supporting structures that both inform and constrain decisions and actions. I account for these structures by modeling them as fellow organization members, fellow decision makers, and IT systems. I also include IT resources and non-IT resources, organizational and groups' tasks as well as representations of organizational and individual knowledge. I constrain the analyses to short-term (e.g., hours to days) measures of performance ([MoP](#)) and measures of effectiveness ([MoE](#)) to compare and contrast conditions under test. I treat modeling and analyses of long-term impacts (e.g., weeks to months) as out of scope while acknowledging such work would be very interesting.

The military organizations modeled in this work generalize to other organizations, but certainly not all, and certainly not to IT dominated organizations (e.g., exchange traded funds ([ETF](#))), or manufacturing lines. As noted above, I limited the research to small sub-sets of the organization, with the expectation that sub-groups may suffer disparate effects to their sub-group missions than the leadership. This may be analogous to a corporate HQ suffering no immediate ill effects from a strike at one of its plants in another state, which has its production rate drop to zero.

The research uses stylized adversaries capable of creating effects in and through the IT systems and IT resources of the modeled organizations. The dissertation also scopes the effects of contested cyber environments (see also [Definitions](#)) to three (3) of the five (5) categories in the Committee of National Security Systems ([CNSS](#)) Information Assurance ([IA](#)) ontology: Confidentiality, Integrity, and Availability. These adversaries, discussed in detail later, are neither omniscient nor omnipotent. The dissertation does not incorporate the remaining two (2) CNSS IA categories of authentication or nonrepudiation.

Modeled adversaries create availability effects against random or specific IT systems within the modeled organizations with varying probabilities of effect. Modeled adversaries can also create availability effects against various technology supported communications mediums in the model (e.g., telephone, classified and unclassified email). The models do not mimic the technical mechanisms an adversary could use to create these effects, nor do I attempt to model and adversarial motive or end-state. The results for the modeled organizations range from no measurable effects to effects high enough to generate a review by the decision makers—statistically significant results will depend on the context . It was not part of the research plan to generate the degenerate case of 100% loss of all communications technology and/or IT systems within an organization.

There is also a set of stylized integrity agents that act, at the various levels of security within the organization models, as spreaders of disinformation. These are abstracted attack vectors without specific implementation techniques in the model. The results from the modeled organizations indicate that various structural configurations speed and slow the spread of disinformation. There are also distinct differences in the longevity of disinformation in decision making circles compared to the organization as a whole.

Finally, I have modeled a passive confidentiality agent as an information sink on the unclassified security level of the models. The intention is to begin the process of understanding how to model confidentiality leaks—though I will not be ascribing specific operational impacts to those leaks (e.g., the impacts of intellectual property leaking to a competitor firm or the designs for modern military equipment).

The short duration cyber environments represent a first step in a long term research plan. It is easy to foresee extensions to this work that would incorporate longer lasting contested environments to trigger and assess more pronounced adaptive and maladaptive behaviors. It is also easy to foresee extensions where attacks incorporate series effects (e.g., attack, pause, attack) as part of a deliberate effort of adversaries to generate adverse environments for organizations under study.

Definitions

Short, plain English definitions are used in this portion of the dissertation with more detailed and thorough definitions in [Definitions](#).

What is a *contested cyberspace* (*cyber* for short) *environment* and why does it matter? Quite simply, a contested cyber environment is a human-built complex system. It includes interconnected telecommunications and information technology networks and network-enabled devices. Most importantly the technology intertwines with people and man-made and natural processes that can, and do, interfere with the designed and intended purpose of the environments. I'll address the 'why it matters' portion of the opening sentence shortly.

The United States Air Force ([USAF](#)) developed a nondoctrinal definition of *mission assurance* that means the USAF and its units can “fight through an attack” (Elder, 2008; Webber, 2010) (see also the definition of [Mission Assurance](#) on page 1-2). Importantly, the decision makers that developed this approach were not information security ([INFOSEC](#)) or computer security ([COMPUSEC](#)) practitioners but were operations generalists. Those generalists, by long experience and exposure, have learned the complex choreography of the USAF's many missions has a central core: successful execution of military operations. The situation is akin to organizations (e.g., oil exploration) that have multiple subordinate elements (e.g., Human Resource ([HR](#)), Finance, Logistics) that perform necessary, even critical functions, that remain, fundamentally, not the primary *raison d'être* of the organization. This USAF concept of mission assurance gives its leadership confidence that it can perform its core and essential supporting missions in the face of adverse circumstances. They develop this confidence predicated on the expectation of future events. This expectation aligns with the right side of [Figure 1](#) labeled *Event Management* that illustrates risk reduction with operating through adversity.

[Figure 1](#) depicts mission assurance as an abstract aggregation of two major components: (1) Iterative application of one or more risk management frameworks; (2) event management. It is important to note that in event management has at least three components: (1) Pre-event rehearsal(s); (2) adaptation during and possibly after the event; and (3) post-event recovery. In the figure, I have also made explicit the need to record and learn from the preceding events—deliberately choosing to not learn lessons qualifies as a maladaptive practice that is beyond the scope of this work.

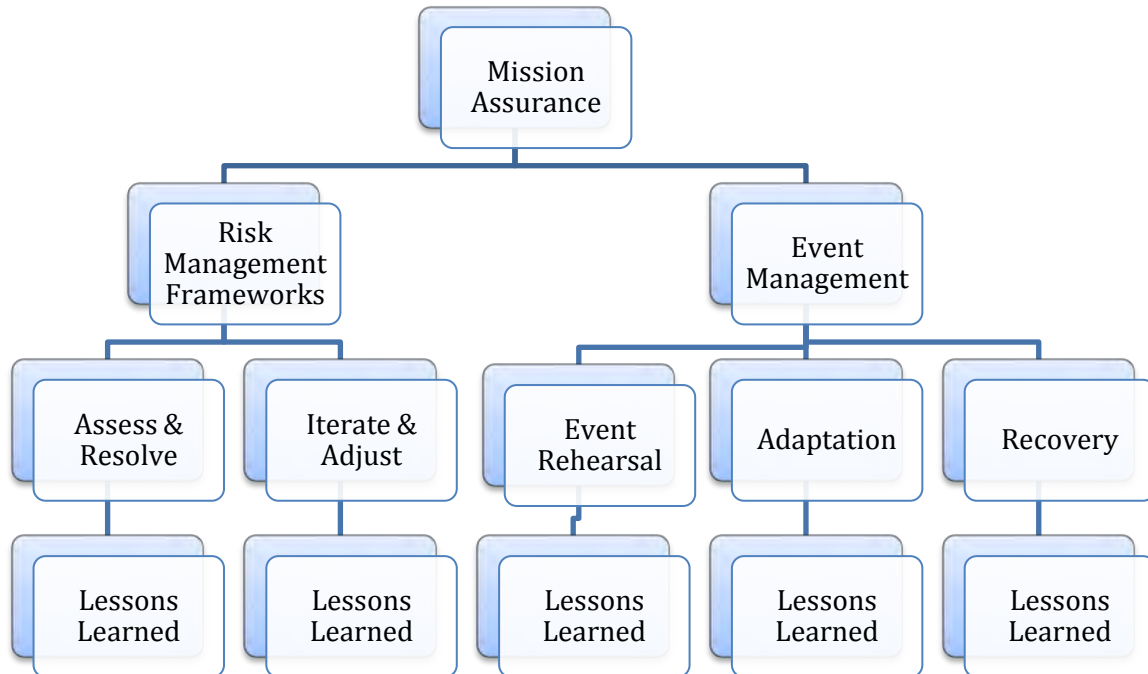


Figure 1: Mission assurance is more than risk management

This continued functioning in the face of adversity leads us to our next, related definition. One way of assessing mission assurance is by leveraging the concept of *resilience*. According to Merriam-Webster’s dictionary, resilience is “an ability to recover from or adjust to misfortune or change” (resilience, 2012). This dissertation applies the definition in two ways: one through a new mathematical definition as a function of congruence between an organization’s requirements, needs, and spare capacity; the second, applied to multiple measures of interest, is the time to return to equilibrium after disruption.

A visualization of the disruption of this new metric, and various other measures of interest is shown in [Figure 2](#) (see also the more complete discussion in the [Network Analytics and Resilience](#) chapter starting on page 118). There are pre-event measures, one or more events, post-event degradation of the chosen measures, and recovery in some fashion. Implicit in this figure is there is a pre-event equilibrium, and there is survival—resilience for stochastic measures cannot exist nor can it have a definition in the absence of survivability.

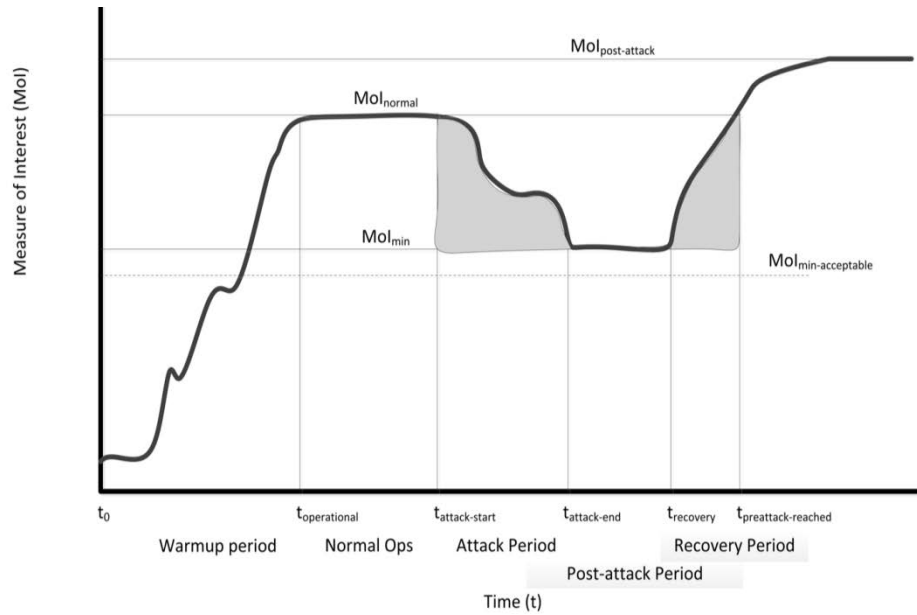


Figure 2: Dynamic visualization of resilience for an arbitrary measure of interest (MoI) ¹

The just discussed motivator of “contested cyber environments” scopes the dissertation to the type of adversity, as does focusing on organizational resilience. Of the multiple ways to model and simulate a contested cyber environment, I simulate abstract mechanisms instead of specific re-creations of named adversaries, technical activities or specific implementations of what the Department of Defense ([DoD](#)) defines as *computer network attack* ([CNA](#)) (Joint Staff J7, 2010a) and have changed (circa 2012) to offensive cyber operations ([OCO](#)).

Actions taken through the use of computer networks to disrupt, deny, degrade, or destroy [emphasis added] information resident in computers and computer networks, or the computers and networks themselves.

The Committee of National Security Systems ([CNSS](#)) definition of *information assurance* helps in this decision by creating an ontology with five (5) effects labeled confidentiality, integrity, availability, authentication, and nonrepudiation ([CIAAN](#)) (2010). I use abstracted mechanisms that create one or more of the first three effects (i.e., [CIA](#)) based on an assessment that negative effects that start in the authentication and nonrepudiation categories often serve as waypoints en route to deliberate effects within the first three categories. When combined together, the use of abstract mechanisms and the CIA ontology supports rapid modeling of effects rather than the specific technical modeling of SYN flood

¹ (Morgan & Lanham, 2012)

denial of service ([DOS](#)) attacks , distributed DoS ([DDoS](#)), cryptographic or message replay attacks, or other specific forms of CNA .

Why is this important?

Since the birth of the integrated chip, there has been an incredible growth in the ways humanity has put IT to use. Though there are still elements of humanity that remain largely untouched by electricity as well as information technology, it's the electricity and IT using organizations that interest us in this research. The growth of the penetration of IT in everyday lives should be fairly noncontroversial, with [Figure 3](#) (on page [12](#)) through [Figure 7](#) (on page [14](#)) depicting examples of growth in civilian and military use of information technology. With the growth in use, there is an accompanying rise in risk that disruption of IT can negatively affect the people and organizations accustomed to its presence.

Returning to the two parts of mission assurance in [Figure 1](#) (on page [6](#)) leaders plan and work to reduce their organizations' various risks as well as plan their reactions to misfortune and adversity. In virtually every risk management framework, a recurring task for organizational leaders is assessing and adjusting framework compliance and adherence measures. Such activities however are beyond the scope of this research effort.

Missing in many of risk management frameworks however are explicit acknowledgements and deliberate planning and rehearsal for the actual occurrence of risk events. Deliberate planning and rehearsal is an implicit acknowledgement of non-zero risk, and a solid foundation for leaders and subordinates alike to increase confidence in mission assurance. Incorporating lessons learned from previous assessments and events is also salutary to increasing perceptions of mission assurance. Short of rehearsing for or living through adverse events, there are other tools available for organizations to increase their perception of mission assurance—specifically socio-technical simulations that support forecasting efficacy of planned mitigations and reactions.

Another shortfall in many risk management frameworks is the oft-repeated phrase that the assessments are snapshots in time. This shortfall becomes problematic when reflections of the organization from weeks, months or years ago conflict with leaders' perceptions of *now*. Rapidly constructed socio-technical simulation models help reduce the

gap between perceptions of now and snapshots of the past, as well as speed contingency planning.

With increased use of IT, leaders of organizations (Loveland & Lobel, 2012), as well as national and military leaders (Lynn, 2010), have assessed there are increased risks to their organizations' ability to adequately perform missions in contested cyber environments. The President of the United States issued Homeland Security Presidential Directive 7 ([HSPD-7](#)) that specified 31 policies the executive branch would pursue to protect assets from all manner of threats—including cyber threats (2003). For all of these leaders, human adversaries are not the only concern with respect to their reliance on cyberspace capabilities. Natural phenomena can also inflict the effects of a contested cyber environment—a degradation, denial, disruption, or destruction of cyber/IT assets. Hurricane Katrina (Piper & Ramos, 2006) and Super Storm Sandy (Carew, 2012) degraded communications for consumers, emergency services, and governmental entities quite extensively. Undersea events from earthquakes to dragging anchors can break undersea fiber optic cables—inflicting both total and partial loss of availability (Niccolai, 2008; Rotenburg, Schneier, McConnell, Zittrain, & Donovan, 2010). Man-made threats to cables include advanced submarines and technology that support eavesdropping (Sherry, Drew, & Drew, 1998; The Associated Press, 2005) to vandalism or sabotage (Reardon, 2009; Shin & Garske, 2012) that can inflict losses of confidentiality and availability on those who use the undersea cables.

Organizations with missions enabled by, or outright reliant on cyber resources, face some amount of risk that the organizations could fail at those missions in a contested cyber environment. IT-enabled supply chain dependent organizations can suffer sufficient degradation or disruption that they are unable to continue their manufacturing, selling, or other missions and may cease to operate (Min & Zhou, 2002; G. E. Smith, Watson, Baker, & Pokorski Ii, 2007). Organizations that are less reliant on IT for their primary day-to-day operations may find that they are less able to conduct other forms of business or operations as well as their secondary functions (e.g., accounts receivable, accounts payable, shipping and receiving, and timely resupply to subordinates, peers, or customers) during periods of contested cyber environments. IT-reliant organizations such as electronically traded funds ([ETF](#)) may also cease to operate, cease to exist due to monetary losses, or otherwise suffer such degradation they cannot sustain their business model—though these types of

organizations are beyond the scope of this work. Targeted attacks against network-enabled supervisory control and data acquisition ([SCADA](#)) can affect organizations that use SCADA such as electric power companies. Degraded SCADA systems could potentially trigger cascading failures such as the 2003 electrical black out in portions of the U.S. and Canada (U.S.-Canada Power System Outage Task Force, 2004). The risks of cascading failure rise with increased interconnections between organizations when those interconnections lack physical and procedural safeguards.

The proceeding paragraphs of this section, in abbreviated form, make the case that the effects of a contested cyber environment can be adverse to organizations' ability to perform their missions or business operations. Such outcomes are contrary to fundamental business interests, and for militaries could hinder the ability to defend or assert national interests. Given that risks of contested cyber environments are unlikely to be zero, there is a prima facie case that leaders should be confident in their organizations' ability to adapt and operate despite such environments.

What will this dissertation do?

There are three broad sets of deliverables within this dissertation, listed in [Table 1](#). The first is a fine grained approach for rapidly assessing organizational resilience to contested cyber environments. The second is a theory of command-level resilience to those environments. The third is a reusable, empirically grounded agent based dynamic network model and associated methodologies for assessing the command-level resilience to cyber attacks and events.

Table 1: Three primary sets of deliverables

Develop a fine grained approach for assessing organizational resilience
Develop a command-level theory of resilience to contested cyber environments
Develop a reusable, empirically grounded agent based dynamic network model and associated methodology for assessing command-level resiliency to cyber attacks & events

Literature Review

Introduction

Mission assurance, having a level of confidence in the resilience of an organization, its ability to recover from or adjust to cyber events, along one or more measurable dimensions is necessarily a multi-disciplinary effort. This literature review expanded from those topics depicted in [Figure 1](#) to include areas of interest as diverse as emergency management, high reliability organizations ([HRO](#)), organizational behavior and learning, supply chain management ([SCM](#)), cyber security, modeling and simulation ([M&S](#)), SNA and network science. Each of these research areas have information and results that can shed light onto each other's areas of interest as well as this dissertation. The review also incorporates research from cyber specific risk management.

This section illustrates the gaps in the literature regarding organizational resilience especially to contested cyber environments as well as need to improve the application of M&S to help cross the gaps. The review will reinforce the links between the research areas that the authors within the corpus identified as well as illustrate the need for more links between research areas that share common areas of interest without normally overlapping.

Increasing use of Information Technology *IT* in many civilian industries and organizations

Since the creation of the integrated circuit, there has been an incredible growth in the ways humanity has put IT to use. Though there are still elements of humanity that remain largely untouched by electricity as well as the information technology, it's the electricity and IT using portion that interests us in this literature review. Two indirect indicators of the growing use of IT within civilian infrastructures are the growing demand and use of the radio frequency spectrum as well as the sales of computer and IT related equipment over the last 35 years. [Figure 3](#) depicts the frequency allocation by the Federal Communications Commission ([FCC](#)) in 2012 with [Figure 4](#) providing the contrast in growth of frequency-use demands. The growth in demand for the various uses of frequencies is a reflection of the growth in the number of ways humanity has put IT to use in our industries and our daily lives.



Figure 3: Federal Communications Commission (FCC) frequency allocation chart circa 2003 ²

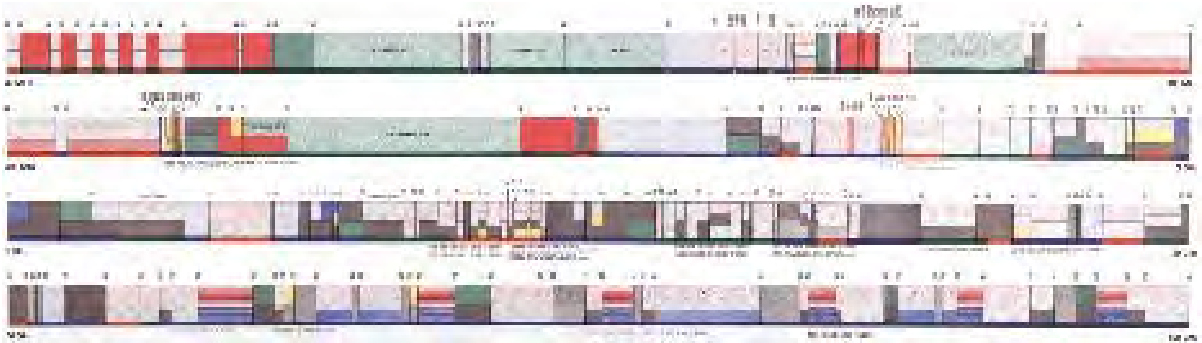


Figure 4: FCC frequency allocations circa 1975 ³

A second indicator, and there are too many possible indicators to enumerate even a tiny fraction, is the sales growth of computers from their inception with ENIAC in 1946 (Weik, 1961) to 2012. There is an apocryphal story that IBM's Tom Watson, Jr., opined he foresaw a market for about 5 mainframe computers in the world in the 1950s⁴, while Gartner forecasted over 400 million computers shipping around the world in 2012. [Figure 5](#) reflects sales growth for personal and desktop computers, with [Figure 6](#) depicting the growth of super-computers—the nearest analog to Watson's mainframes that was IBM's core business through the 1980s. The figure is depicting the distribution of super-computers across the continents of the globe, and limited to the top 500 super computer systems—the entry level has moved up to 76.5 teraflop (Tflop)/s (floating point operations per second) from 60.8 Tflop/s in May 2012 (Meuer, Strohmaier, Simon, & Dongarra, 2012)

² (US Department of Commerce, 2003)

³ (Elder, 2008)

⁴ IBM asserts this story is a misunderstanding of statements made by Tom Watson, Jr., in their Frequently Asked Questions (FAQ) (IBM, 2007)

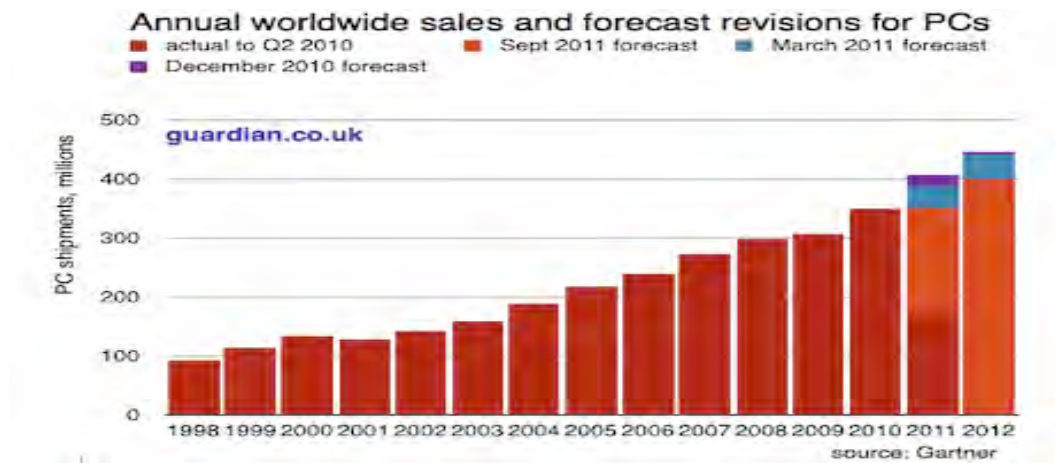


Figure 5: Sales growth for personal computers from 1998 to 2011⁵

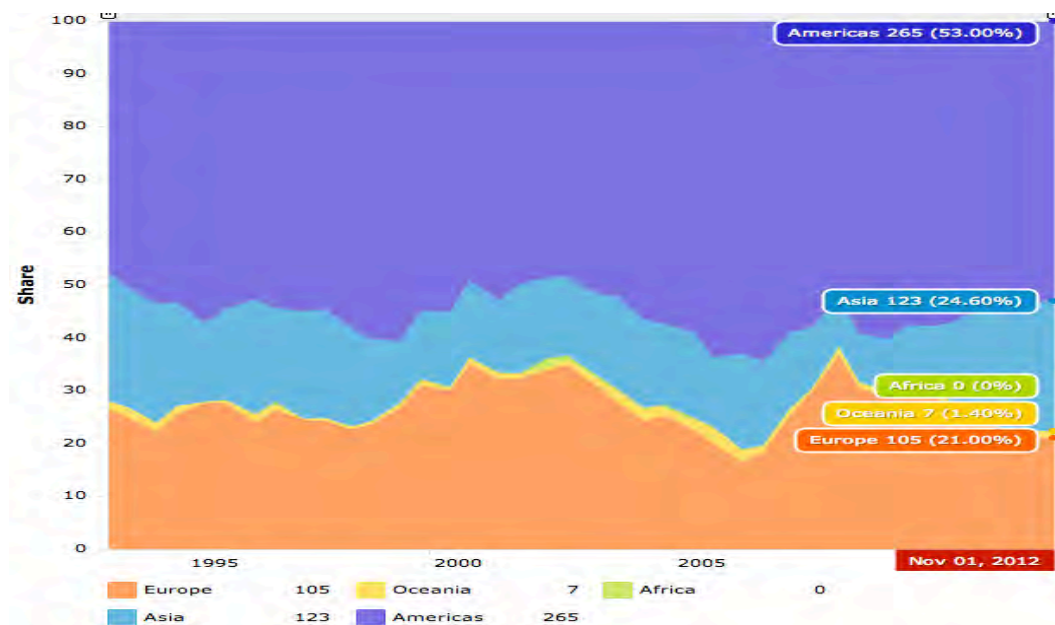


Figure 6: Growth in installed super-computers by continent since 1994⁶

Increasing use of IT by US Department of Defense (DoD)

The DoD's growing division of the frequency spectrum also reflects this growth in frequency requirements. US military forces are, in some respects, the most IT-enabled military on the planet with their blue-force-trackers, remotely piloted aircraft (e.g. Predators, Global Hawks), small unit access to real-time streaming video of their area of operations, as well as line of sight ([LOS](#)) and beyond line of sight ([BLOS](#)) encrypted radios. Such is the extent of infiltration of IT, that the White House situation room had as-it-happened

⁵ (Arthur, 2011)

⁶ (Meuer, Strohmaier, Dongarra, & Simon, 2012)

information sent around the globe from Pakistan during the raid to kill Osama bin Laden (Souza, 2011). [Figure 7](#) is a DoD specific chart depicting the use of the radio frequency ([RF](#)) spectrum that, while not all-inclusive, is a reflection of the number of uses for the RF spectrum that simply did not exist 35 years ago (e.g., Global Positioning System ([GPS](#)), Unmanned Aerial Vehicles ([UAVs](#)), Defense Satellite Communications System ([DSCS](#)), and Mobile Subscriber Equipment ([MSE](#))).

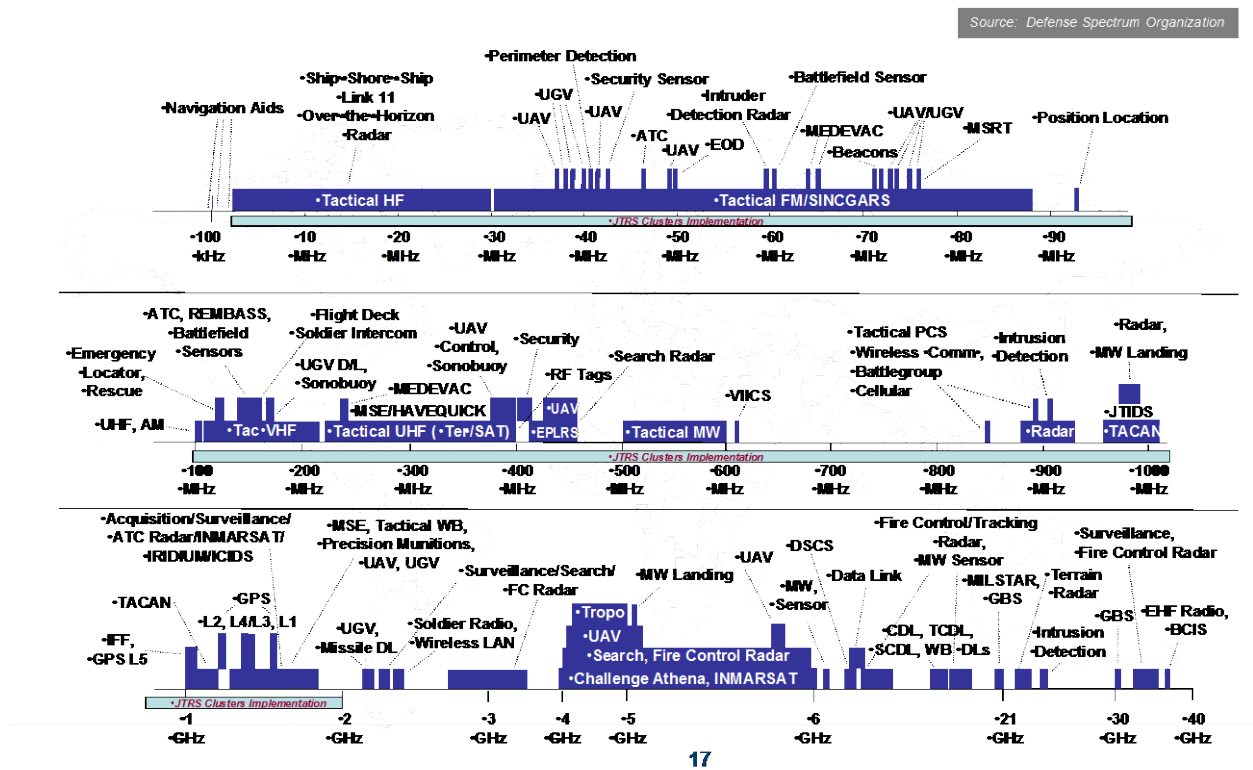


Figure 7: US DoD frequency allocation chart circa 2010 ⁷

Increasing risks from contested cyber environment

With increased use of IT, leaders of organizations (Loveland & Lobel, 2012), as well as national and military leaders, are assessing there are increased risks to their ability to execute their missions despite contested cyber environments. Former Deputy Secretary of Defense William J. Lynn III, among many others, has published his belief that the very advantages IT systems give the US, potentially allow adversaries of all kinds anti-US operational opportunities. Those opportunities can range from disrupting US logistics support to operations around the globe as well as degrading the perception of control of globally

⁷ (Defense Business Board, 2010)

deployed forces by national leaders (Lynn, 2010). The President of the United States ([POTUS](#)), also growing concerned about the perceptions of risks to ‘critical infrastructure,’ issued HSPD 7 that enumerated 31 policy positions that the executive branch would pursue with respect to protecting assets from all manner of threats—including cyber threats (Office of the President of the United States, 2003).

Human adversaries are not the only concern for the national leaders around the globe. Natural phenomena can also inflict the effects of a contested cyber environment—a degradation, denial, disruption, or destruction of cyber/IT assets. Hurricane Katrina (Piper & Ramos, 2006) and Super Storm Sandy (Carew, 2012) degraded consumers’ communications quite extensively, as well as emergency services’ and governmental entities’. Undersea events can also break segments of the global undersea fiber optic cable network—inflicting a loss of availability (Niccolai, 2008; Rotenburg et al., 2010). Man-made threats to undersea cables also include advanced submarines and technology that support eavesdropping on those same cables (Sherry et al., 1998; The Associated Press, 2005)—inflicting a loss of confidentiality. Having leaders that are aware of possible cyberspace related risks is a necessary condition for organizations to take steps to reduce those risks as well as take steps to ensure their ability to operate despite any contestation of their cyber environments.

Contested cyber environments as risks to organizational resilience

Emergency services, HROs, governmental leaders and their staffs are not the only stakeholders contested cyber environments put at risk. Organizations with missions enabled by, or completely reliant on cyber resources, face some amount of risk that the organizations could fail at those missions in a contested cyber environment. Organizational dependency on IT can vary anywhere along the spectrum from no dependency at all to the opposite end where the organization will cease to meaningfully operate without IT.

Organizations that are less reliant on IT for their primary day-to-day operations may face degradation in their abilities to conduct other forms of business, operational, or secondary functions (e.g., accounts receivable, accounts payable, shipping and receiving, timely resupply to subordinates, peers, customers) during periods of contested cyber environments. Organizations dependent on supply chains could suffer sufficient degradation or disruption that they are unable to continue their manufacturing, selling, or other missions

and may cease to operate (Min & Zhou, 2002; G. E. Smith et al., 2007) if the disruption lasts too long. Organizations and business that are, at heart, IT reliant may also cease to operate, cease to exist due to losses, or otherwise suffer such degradation they cannot sustain their business model; exchange traded funds ([ETF](#)) companies can often define exactly how much money they lose during service interruptions and work hard to minimize those potential losses.

Organizations that provide, operate, and maintain the many parts of national critical infrastructure also have some vulnerability to contested cyber attacks through their use of in-band and out-of-band control systems (often called Supervisory and Control Systems ([SCADA](#))). Those and other organizations can also have indirect at risk outside their direct control. Cascading failures of power systems, such as the 2003 electrical black out in portions of the US and Canada (U.S.-Canada Power System Outage Task Force, 2004) represent a class of indirect risk. Where interconnections between providers of any cyber related service exists, degradation or disruption of one or more providers may, like electrical distribution systems, cause a shifting of load to other elements of cyberspace—those elements may or may not be capable of supporting the new demands.

Related Areas of Research

What does resilience mean?

What is resilience? Revisiting Merriam-Webster, it is “an ability to recover from or adjust to misfortune or change” (resilience, 2012). There are variations on this definition that scope the definition to ecology and life sciences fields. The physics community has a definition of resilience as the potential energy stored in an elastic material when the material is deformed (resilience, 2003). When applied to technical systems, and in particular systems of systems, some definitions add language that requires recovery be to the level of performance or measure of interest present prior to the event (Bishop, Carvalho, Ford, & Mayron, 2011). Other definitions require the system(s) of interest be able to predict disruption (Pflanz & Levis, 2012), and that the system will function as the owners ‘required and intended’ (Horning, 2009) despite being in a hostile environment.

Still others perceive resilience as a series of traits (Coutu, 2002) that companies and assessments must then operationalize by converting the traits to measures of performance

([MoP](#)) and measures of effectiveness ([MoE](#)). Gunderson asserts that resilience, is effectively “magnitude of disturbance that can be absorbed before the system redefines its structure by changing the variables and processes that control behavior” and refers to Walker et al calling this “ecological resilience” (Gunderson, 2003).

Resilience Engineering

The variety of definitions, especially applied to systems of humans and equipment has even lead to the establishment of a field of engineering entitled “Resilience Engineering.” Practitioners of resilience engineering view systemic or organizational mishaps as failures to maintain systems, processes, and thought processes as the inverse of adaptability and resilience (Hollnagel, Woods, & Leveson, 2006; Madni & Jackson, 2009c; REA Public Affairs, 2013).

In the resilience engineering domain, the focus tends toward safety as a primary metric. Madni and Jackson collected and synthesized fourteen heuristics in their review of the growth of resilience engineering (2009a) that they break into near-term and longer-term categories: reaction and adaptation respectively (2009c). In a different formulation, Westrum asserted resilience has three meanings: the ability to prevent something bad from happening; the ability to prevent something bad from becoming something worse; and the ability to recover from something bad once it has occurred (2006). Westrum also distinguishes coping by being adaptive (e.g., organizations changing themselves in response to a crisis) and being armored (e.g., a tank) (2006). Both examples reflect different approaches to survivability with one being very hard, and very resistant to minor perturbations. Unfortunately, once disruption reaches the tank-armor’s breaking point, catastrophic failure is the typical, and often unsafe, outcome. This opposite state of resilience has earned the label brittleness (Hollnagel et al., 2006; Madni & Jackson, 2009c).

Why resilience to contested cyber environments?

This literature review will limit the scope of reviewed adversity to the effects of contested cyber environments wherever feasible, though there is a surprising paucity of research that restricted itself to IT based adversity or even passingly referred to IT based adversity. In addition to this dissertation, other researchers have taken note of the dearth of research into cyber effects (Chapman, Leblanc, & Partington, 2011; Leblanc, Partington,

Chapman, & Bernier, 2011). Enumerating or creating ontologies of specific origins of threats (e.g., insider/outsider, malicious/nonmalicious, natural/manmade) is certainly a time honored way of problem decomposition for cyber security (Bishop, Engle, Peisert, Whalen, & Gates, 2009a, 2009b; Chapman et al., 2011). Clearly the nature of threat(s), their likelihood, and their ability to incur an effect contribute to organizations decisions about resource allocations and residual risk acceptance. Rather than adding to this well developed, and yet still evolving body of research, this dissertation explores the need for organizations to be resilient to the *effects of events in the cyber environment*. Organizations and people must be able to adapt to or otherwise cope with the effects to return to some post event equilibrium. Which effects of contested cyber environments in particular? We will co-opt three of the five pillars of information assurance: confidentiality, integrity, availability, authentication, and nonrepudiation (CNSS, 2010) as the effects of interest.

In some research or operations circles, this focus on the effects of cyber environments could fall under the label of ‘effects based operations’ ([EBO](#)) (P. K. Davis, 2006). I will not be exploring this application of the EBO label. Indeed, this focus on effects defers to other authors the comprehensive discussions of how contested environments come into being. Readers will not see in this dissertation details and explorations of the manipulation of bits, bytes, protocols, buffers, and other technology-oriented discussions on how to create contested cyber environments nor the efforts to identify appropriate targets to achieve desired objectives.

Organization adaptation and learning

Generalized discussions of resilience, the ability of both people and organizations to improvise (a key trait identified by Coutu (2002) and Madni (2009a)) and adapt to adversity are useful for developing perspectives and theoretical frameworks for organizational resilience. Fundamental to the idea of adaptation to adversity is the idea that organizations are capable of learning new behavior in the first place (Gunderson, 2003). It is clear from observation that organizations can learn—lists of companies, and even countries that modify their behavior over time would be long, and filled with varying levels of success from survival through flourishing. The inverse is equally true, the history of humanity is replete

with sovereign entities, countries and companies that have ceased to exist—arguably through their inability to adapt to changing conditions.

What motivates or provokes those changes, the adaptation, and learning? There are three longstanding observations of organizational learning, also shown in [Table 2](#). The first observation is organizations base their behavior on routines, on their collective perception of organizational history, and on their goal orientation (Crichton, Ramsay, & Kelly, 2009; B. Levitt & March, 1988). The second observation is behavioral changes occur through positive and negative feedback loops, especially distinctions between perceptions of success and failure, as well as incremental modification of routines (B. Levitt & March, 1988; Norris, Stevens, Pfefferbaum, Wyche, & Pfefferbaum, 2008). The third observation is those organizations’ self-perceptions of being adaptable, of being able to cope with the variations of every day requirements as well as manage unusual circumstances are a key component of making the belief a reality (Dutton & Dukerich, 1991). Knowing the above, the reader may be wondering what then inhibits organizational learning and adaptation?

Table 2: Three observations on organizational learning

Organizations base their behavior on routines, on their collective perception of organizational history, and on their goal orientation
Behavioral changes occur through positive and negative feedback loops, especially distinctions between perceptions of success and failure, as well as incremental modification of routines
Organizations’ self-perceptions of being adaptable, of being able to cope with the variations of every day requirements as well as manage unusual circumstances are a key component of making the belief a reality

There are at least three structural difficulties in learning from experience identified in research: paucity of experience, redundancy of experience, and complexity of experience (B. Levitt & March, 1988), shown in [Table 3](#) below. Without experience in a degraded environment to establish routines, fail-over plans, and without a perception of “we’ve done this before,” an organization has not learned the true effects of a degraded cyber environment to their particular situations. The situations they could face are each a possible source of creating routines the company switches to in contested cyber environments.

The success versus failure ratio can only change with modifications to its numerator or denominator. Behavioral psychologists have long known that repetition is a key component of learning for individuals, and repetition is the key to adjusting the

organizational perception of success: failure ratios for given scenarios or general sets of circumstances.

The third component of organizational learning, as well as the third challenge set the stage for non-trivial exercises and rehearsals. The natural state of IT-based capabilities for many users is that there is ‘always’ something going amiss with their tools, networks, or other IT-based capabilities. But without shifting from the aperiodic, noncatastrophic, low-duration, nonpervasive outages of ‘normal,’ organization members will face unexpected complexities and potentially lose their own perception of adaptability—they are akin to the Westkin’s armored tank where the energy resistance capacity of the armor is exceeded and catastrophic results occur.

Table 3: Structural challenges to organizational learning

Paucity of experience
Redundancy of experience
Complexity of experience

This perception of adaptability is a point of pride for the various US Armed Services—virtually every US Army and US Air Force Posture Statement in the last fifteen years has specifically called out adaptability, learning or transformation (Office of the Chief of Staff of the U.S. Air Force, 2012; Office of the Chief of Staff, 2012). Each Service also embodied adaptability in the creation of new doctrine in the 1980s (Romjue, 1984) and 1990s.

Incident and event response and rehearsal

Many United States Government ([USG](#)) documents call for better and more preparedness for using IT and other cyber capabilities to offset declining budgets and resource levels, increase efficiencies, and increase efficacy of available resources. These documents often advocate for the defense and sustainment of existing and future IT based capabilities. What the documents omit, with some recent exceptions such as (Kaminski, Gosler, & Von Thaer, 2013), are directives to leaders to train and practice their missions within degraded environments—what the US military often refers to as specified tasks in contrast to implied tasks. One outcome of this lack of deliberate training in degraded environments is leaders are training for environments with incompetent adversaries while blithely assuming defeat of attacks or rapid restoration of lost assets (Lanham, 2012c). The

omission also reinforces all three structural difficulties in learning from experience: paucity of experience, redundancy of experience, and complexity of experience (B. Levitt & March, 1988). Indeed, the dominant tone of many cyber related government documents is fear of the loss of IT and cyber capabilities with few, if any, references to the requiring reasonable preparedness and expected adaptation to the destruction, disruption, or degradation of cyber resource. Without loss of IT or degradation of IT training to construct lessons, the palpable fear by reporters and luminaries in the open press could simply be another example of propagating disaster myth (Norris et al., 2008; Tierney, Bevc, & Kuligowski, 2006)—the sky will fall without our necessary IT.

This section has presumed that leaders and organizations recognize they have entered a purposeful contested cyber environment. This presumption is not always true, and indeed, the majority of mass media reports indicate companies learn they have been attacked well after the attack began, especially in the case of advanced persistent threats (APT), industrial espionage, and intellectual property theft. Two frequent ways organizations learn of an APT in their midst is from external reporting (e.g., FBI) or a system administrator chasing down an anomalous bit of behavior. Anecdotal stories abound of leaders reporting they had no idea they were under attack, they had presumed [the technology problems] were related to other causes, not deliberate actions by hostile actors.

Though I found no evidence of conscious effort to avoid purposeful and meaningful rehearsal of contested cyber environments, there is considerable effort dedicated within risk management and cybersecurity communities at preventing, or reducing to ‘acceptable levels of risk,’ the occurrence of cyber events. The USG has built an information assurance model of cyber security widely used by the three branches of government, academia, and industry.

Information Assurance pillars

There have been long running efforts by USG entities to fortify and protect their IT systems and cyber capabilities, prominent among them were Department of Defense ([DoD](#)) Directive ([DoDD](#)) 5200.28 *Security Requirements for Automatic Data Processing (ADP) Systems* of the 1980s; which spawned DoD 5200.28-STD *Department Of Defense Trusted Computer System Evaluation Criteria*, aka “The Orange Book” and its accompanying “Rainbow Series.” Efforts continued through the creation of *Common Criteria* of the 1990s,

and DoDD 8500.1E *Information Assurance* encapsulates current DoD efforts. The USG has been making additional strides to implementing effective Information Security through the passage and implementation of the Federal Information Security Management Act ([FISMA](#)) ("FISMA," 2002), which tasked the heads of federal agencies and the National Institute of Standards and Technology ([NIST](#)) to standardize Information Security ([INFOSEC](#)) risk models in support of legislative oversight responsibilities. A portion of the DoD contribution to NIST's standard framework, applicable to national security systems, is a glossary of terms provided by the Committee on National Security Systems ([CNSS](#)) Instruction ([CNSSI](#)) *National Information Assurance (IA) Glossary* (CNSS, 2010). FISMA established three fundamental elements to the notion of information security: integrity, confidentiality, and availability.

CNSSI No. 4009 goes on to add two additional elements to the definition of information assurance—a rewording of FISMA's definition of 'information security.' CNSSI 4009 defines each of the five pillars of information assurance as shown in [Table 4](#) below (2010). The Department of Defense's definitions draw from these definitions and sometimes add additional verbiage (Department of Defense, 2007). With these five terms, we can characterize events as diverse as SYN floods or other forms of denial of service attacks to undersea cable breaks as a loss of availability. Replay attacks, injecting false radar tracks into radar systems, and changing the contents of personnel and finance computers all naturally fall under loss of integrity effects. Key logger trojans, universal serial bus ([USB](#)) key-capture devices, account credential thefts all fall first under the effect of compromised or lost authentication, with likely follow-up effects in confidentiality, integrity, and nonrepudiation. It is with the first three of these effects that I will focus the dissertation.

Table 4: CNSSI 4009 definitions of CIAAN

Term	CNSS Definition
Confidentiality	The property that information is not disclosed to system entities (users, processes, devices) unless they have authorization to access the information.
Integrity	The property whereby an entity has no unauthorized modifications.
Availability	The property of being accessible and useable upon demand by those with authorization.
Authentication	The process of verifying the identity or other attributes claimed by or assumed of an entity (user, process, or device), or to verify the source and integrity of data.
Nonrepudiation	Assurance that the sender of information receives proof of delivery and the recipient has proof of the sender's identity. Neither sender nor receiver can later

	deny having processed the information.
--	--

The Five D's—Disrupt, deny, degrade, destroy, and sometimes deceive

With the DoD, discussions of contested cyber environments frequently revert to the four elements within its definition of computer network attack ([CNA](#) referred to as offensive cyber operations (OCO) since circa 2012)—disrupt, deny, degrade, and destroy—and sometimes adds the element of deceive from the definition of Information Warfare ([IW](#)). Literature associated with cyber security and contested cyber environments frequently use these terms, and their definitions are important for further discussions. The DoD's Joint Publication ([JP](#)) 3-13 *Information Operations* (2006), defined these terms as shown in [Table 5](#). These definitions represent different, but neither mutually exclusive nor orthogonal, ways of characterizing contested cyber environments. A visualization of these two characterizations, and how they could overlap in 2D space, is shown in [Figure 8](#). The links represent one way of mapping each of the 5 D's into one or more of the CNSS 5 pillars of IA.

Table 5: DoD definitions of the five D's (2006)

Term	DoD Definition
Disrupt	To break or interrupt the flow of information.
Deny	To prevent the adversary from accessing and using critical information, systems, and services.
Degrade	To reduce the effectiveness or efficiency of adversary C2 or communications <i>systems</i> , and information collection efforts or means. IO can also degrade the morale of a unit, reduce the target's worth or value, or reduce the quality of adversary decisions and actions.
Destroy	To damage a system or entity so badly that it cannot perform any function or be restored to a usable condition without being entirely rebuilt
Deceive	To cause a person to believe what is not true. [Military Deception (MILDEC)] seeks to mislead adversary decision makers by manipulating their perception of reality (Joint Staff J7, 2010a).

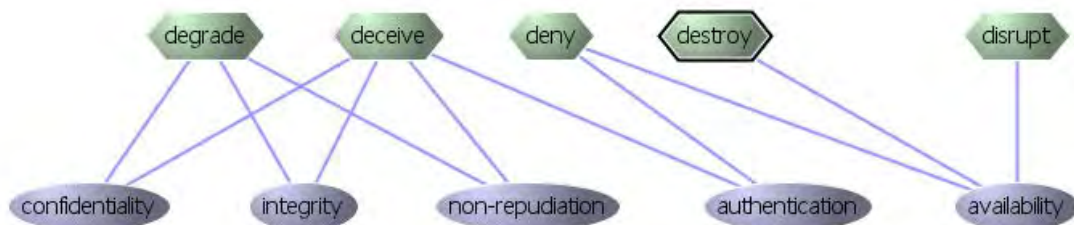


Figure 8: Five pillars of IA and the five D's

Why resilience? Isn't risk management enough?

This section provides a review of the fundamental techniques of risk management. It also establishes that these techniques are insufficient for providing assurance that an organization is resilient to contested cyber environments.

There are four principal tools of risk management, including cyber risk management (Akintoye & MacLeod, 1997; Al-Bahar & Crandall, 1990). The four tools are avoidance, prevention and reduction (also called mitigation), retention, and transfer. But what do organizations perceive as risk (Cashell, Jackson, Jickling, & Webel, 2004)?

Organizations often perceive risk as a set of quantities that they can measure, cost shift, avoid, or otherwise measurably reduce (Flinn & Stoyles, 2005; Wallner, 2008). The downside(s) of those risks have some nominal negative impact on one or more aspects of the organization. The emphasis in traditional cyber risk management is reduction of the problem to one of two fairly simple models represented in equations (1)(MITRE, 2012a) or (2) (Stoneburner, Goguen, & Feringa, 2002).

$$Risk = Probability \ Occurrence \times Impact \quad (1)$$

Equation 1: Risk as a function of the probability of occurrence and the forecasted impact

$$Risk = f(Threat, Vulnerability, Asset) \quad (2)$$

Equation 2: Risk as a function of three variables: threat nature, vulnerability nature, and asset value

Importantly, none of these tools *explicitly* incorporates the notion of resilience: being able to recover from or adapt to the occurrence of a risk event. Resilience requires an explicit acknowledgement that risk cannot equal zero, and that risk varies over time. Mission assurance requires acceptance that nonzero risk means bad things will happen to an organization, despite the various avoidance, mitigation, retention and transfer measures in place. How organizations deal with that adversity is what assures their members and their leaders that cyber adversity is not an existential threat but a threat they can adjust to and function through. Without the explicit inclusion of both the ability to recover and the ability to adapt to the effects of the contested environment, traditional risk management is necessary for but not sufficient to establish mission assurance.

Cyber threat literature

What kinds of threats and problems exist that could create contested cyber environments? The introduction already alluded to at least two categories: man-made and natural. By natural, I'm referring to storms and other weather events, landslides, flooding, and virtually any other event for which humans are not the proximate cause. The other set of threats are man-made. Efforts to categorize these man-made threats, and their alter egos, vulnerabilities, have ranged from the taxonomies presented in the RISOS project (Abbott et al., 1976) to the four overlapping categories of the Protection Analysis project (Bisbey & Hollingsworth, 1978). Bishop built a taxonomy of six axes (1995) through using the categories of the Protection Analysis project as well as modified versions of Landwehr's three categories (Landwehr, Bull, McDermott, & Choi, 1994). Howard's dissertation (1997) has an extensive review of taxonomy attempts including the use of "results Categories" that mimic three of the five CNSS pillars of information assurance (i.e., confidentiality, integrity, and availability) by Cohen, Russell and Gangemi. Howard himself went on to develop what he called a process model whereby attackers use tools, to gain access to cyber systems, to create results to achieve some objectives (Howard, 1997). Hansman, like Howard, broadened his taxonomy to address specific vulnerabilities as well as three other dimensions of attack: vector, target, common vulnerability and exposure ([CVE](#)) entries, and payload or effect beyond the attack itself (Hansman & Hunt, 2005).

There are at least two degenerate cases of threat in the cyberthreat literature: (1) the nonexistent threat, in which case [Equation 2:](#) will equal zero (0); and (2) the computationally all-powerful adversary such as the Dolev and Yao adversary (1983) where the outputs of [Equation 1:](#) and [Equation 2:](#) are always greater than 0, and implicitly $\gg 0$ while still ≤ 1 . More interesting are the arguments put forth that adversarial assumptions can lead to significant gaps in theoretical modeling (Gligor, 2008) and subsequent faulty policy decisions. Such arguments assert that adversary models should include the capabilities and resources available as in (F. Cohen, 1999; Leblanc et al., 2011) as well as include adversary's motivations (Gligor, 2008; Parker, Sachs, Shaw, & Stroz, 2004).

The efforts to classify and categorize cyber threats remain areas of continuing interest for a variety of audiences, researchers, and the military; Sun Tzu noted that knowing your enemy is essential to becoming a victorious general (2003). The intention in the preceding

paragraphs was to illustrate a small portion of the efforts spent in that line of research—a complete rendering is well beyond this dissertation and not entirely beneficial to the point of focusing on the effects of contested cyber environments, independent of the agents and motivations of those agents.

Rhetoric of catastrophic vulnerability

There is hardly a week that goes by in the last several years when yet another news story discusses yet another cyber attack against some entity somewhere. Former US Defense Secretary Panetta is part of a long list of high USG official warning of dire threats to the US from “aggressor nation or extremist group” actors (Bumiller & Shanker, 2012). He is by no means alone, with the head of the National Security Agency and the new Cyber Command, General Alexander (Alexander, 2012; Roulo, 2012), the former Deputy Secretary of Defense Lynn (Lynn, 2010), and even the President of the United States all asserting that cyber security is a national security challenge with grave consequences if the country gets it wrong. Some US government representatives are less circumspect in their comments and conflate cyber attacks with an existential threat to the country (Thibodeau, 2010), feeding into a leader and media fed meme—dependence on IT equates to a loss of modern civilization if IT is degraded; a meme similar to the disaster myth of (Tierney et al., 2006).

These warnings may be rhetorical flourishes to overcome bureaucratic inertia, sincere efforts at forecasting the future, or simply appeals to historical analogy. In assessing the rhetoric, it is useful to ask, “What have been the outcomes of past events that had effects in the cyber domain?” “There are various estimates of monies lost from cyber enabled financial crimes (Cashell et al., 2004; National White Collar Crime Center (NW3C), 2011), cyber enabled copying or destruction of intellectual property (Andrijcic & Horowitz, 2006; Nykodym, Taylor, & Vilela, 2005; G. S. Smith, 2004). There are national security estimates about years shaved off nation states’ research programs thanks to stolen plans from US companies (Gorman, Cole, & Dreazen, 2009) and government agencies (Abreu, 2001; Kan, 2006). There are even reports of long-term attacks that copied unknowable amounts of data for which effects may never be known (Lennon, 2011; Perlroth, 2012; Thornburgh, 2005). What are the after effects of these and other reported events, aside from the prima fascia effects of monetary loss?

Cyber effects and strategic war fighting

There are public figures, pundits, authors, and former government officials, who declare that cyber war is already a reality. Richard Clarke's book *CyberWar* is one example of such. But there is significant countervailing opinion—that not only is cyber war not here yet, but that the very word is a misleading and inappropriate conflation of distinct ideas. Security professionals such as Bruce Schneier and Marc Rotenburg concede that enormous quantities of cybercrime and espionage happen, but emphasize that though the threats are real, they are not war threats (Rotenburg et al., 2010). Despite the almost palpable fear in the testimony by General Alexander, Director National Security Agency ([DIRNSA](#)) and Defense Secretary Panetta's public speeches, there are significant doubts that any enemy's cyber capabilities can inflict significant long-term effects on the US—with equal doubts about US means to use cyber capabilities to war ending effect (Economist Editorial, 2012). It would not be the first time that pundits proclaimed that a technology represented a revolution in military affairs that makes warfare history irrelevant to the vision of future war—examples range from cross bows, to guns, to machine guns, to airplanes and long-range bombers, to nuclear bombs/missiles. The means change, decision requirements and information flows expand and contract, response times increase or decrease, but war continues, regardless of the perceived overwhelming technology edge of one side or another.

Impacts of past large scale cyber-affecting events

There is much gnashing of teeth in US defense circles about the speed with which China generated its modern stealthy fighters—especially after media reports of copied data moving from US defense contractors to China (Gorman et al., 2009; Reed, 2012; Staff Writer, 2012c). The Chinese creation of such a plane was not a matter of if, but of when. No technological advance, once exposed to the rest of the world, stays long in the sole possession of its creators. Creators execute the hard and expensive scientific efforts of proof of possible; copyists execute the efforts for reproduction and imitation. The concerns over Moonlight Maze (James Andrew Lewis, 2010), Titan Rain (James Andrew Lewis, 2005; Thornburgh, 2005) and subsequent named intrusion sets into US government computer systems are also widely reported, frequently talked about, and yet rarely with specificity or even convincing generality. There are multitudes of mass media reports that USG cyber capabilities are infiltrated across the breadth of its unclassified systems—but if reports exist

about the specific impacts of that infiltration, they are certainly not available to convince the general public of the harm done. Without the data points of harm done, it becomes difficult to assess the plausibility of the extrapolations of catastrophic impacts in the future. Indeed, the most recent report from the US Director of National Intelligence ([DNI](#)) reported the likelihood of a catastrophic attack is ‘remote’ and forecasting has now shifted to less grandiose outcomes {Clapper, 2015 #7696}. Surely secrets have been lost, spies likely killed, citizens of countries imprisoned, but no credible argument has been made that those events would not have happened if all were quiet on the cyber front.

Degradation in cyber capabilities, and, sometimes, outright destruction of support infrastructure, are almost signature marks of modern large storms making landfall on our coats. Hurricane Katrina and Super Storm Sandy both offer possibly instructive insights as to the cyber effects of natural environments. In Hurricane Katrina, of the many troubles faced by emergency management services, widespread loss of electricity as well as intermittent and total loss of communications are prominent in lessons learned reports (Guilford, 2010; Townsend, 2006). None of these reports point out loss of cyber and IT capabilities as a proximate cause of fatalities. None of these reports claim restoration of cyber capabilities would have significantly reduced the near term impacts of Katrina. The long-term health and demographic impacts New Orleans is still living with are several causal links away from cyber capabilities in the region—so the case for long-term effects of contested cyber environments has yet to be convincingly made to warrant the perceived levels of dread.

Super Storm Sandy’s impacts on emergency and other governmental services were equally profound in the short term. And despite the loss of electricity to over 7.9 million people (CBS/AP, 2012c) for days, and in some locations, even weeks (CBS/AP, 2012a), there are no lessons learned reports yet making the claim that a faster return of cyber and IT capabilities would have substantially reduced the widespread and long-term impacts of the storm. The loss of electricity, and other forms of damage, also impeded the reopening of mass transit systems (McCoy, 2012) that served millions of people a day (Goldman, Klopott, & Vekshin, 2012). There has not been a credible declaration that their complete stoppage for days, and only partial reopening, had destroyed New York, New Jersey and other served areas—so exactly what would the long-term effects be of a SCADA attack on mass transit systems? Water and sewage systems in shore communities from New Jersey (Reporter, 2012)

to Connecticut (WFSB Staff, 2012) were negatively affected as well by the storm through loss of electricity, flooding of facilities, uncontrolled spillage of untreated sewage into waterways (Schwartz, 2012). Again, no credible declarations of long-term catastrophic damage to those communities from storm impacts to those utilities exist. This drives the question of exactly how would a [SCADA](#) based attack on water and power systems degrade our civilization?

Finally, there is a set of fears that large-scale cyber attacks could dramatically and negatively impact the country's and global financial markets. Prima fascia evidence is usually from the Estonian attacks of 2007 (Ashmore, 2009; J. Davis, 2007), the Georgian (Clark & Levin, 2009) and Lithuanian attacks of 2008 (Ashmore, 2009). On further review however, the effects were greater in the public psyche and government outlook than in actual damages to citizens or organizations within those countries. Enumerated damages included delays of hours for monetary transactions and days for newspaper and government information diffusion—hardly the cataclysmic outcomes of popular myth (Ashmore, 2009).

The closures of the NY-based markets from the 2003 power outages (Barron, 2003; SEC, 2003), the 9/11 attacks (Masi, Smith, & Fischer, 2010), during and post Sandy (Kim, 2012) all had measurable impacts (e.g., [USD](#)1.7 trillion in market losses (Navarro & Spencer, 2001)) and were more pervasive than any cyber attack thus far. However, the markets opened, organizations that existed prior to those closures existed after the closures (with some obvious exceptions of those housed exclusively in the twin towers), companies earned money, paid taxes, and wrote off losses. In fact, there are precious few reports of public companies driven to bankruptcy or other ruin due to cyber events—so exactly what are the long-term effects of contested cyber environments?

In 2008 there were a series of undersea fiber optic cable breaks that decreased regional bandwidth by 75% and in some instances logically isolated portions of the global cyber communications networks (Masi et al., 2010). During that time, the US had major combat operations on going in two theaters of war, and countries in the effected region were in the midst of conducting their routine international trading and running their national economies. Far from being unusual, undersea cable breaks are common, so much so that repair ships can spend 11 of 12 months a year at sea (Pole, 2009). With millions of end users,

tens of thousands of organizations (governmental, public, and private), and dozens of countries effected (Masi et al., 2010), no country's government has fallen, no stock markets suffered long-term crashes, no populations panicked into barbarity, and not a single war was started or ended due to loss of those capabilities. These breaks serve to create denial of availability and disruption of communications, but otherwise appear to generate little to no global effects and little to no long-term regional or local effects. The lack of empirical evidence of local or regional collapse, strongly suggests that extrapolations of catastrophic impacts are, at best, unsupported by evidence and at worst are appeals to fear of the unknown.

Appeals to analogical reasoning—cyber Pearl Harbor, Maginot Line, etc.

There is an obvious analogical fallacy in attempting to rally preparedness for contested cyber environments with a call to avoid a “Cyber Pearl Harbor.” The Japanese attack on Pearl Harbor had immediate and obvious effects such the death of over 2,400 sailors, soldiers, and marines, the sinking or damaging of 21 ships, and the destruction of over 180 aircraft (Staff Writer, 2012a). That strategic surprise (at least to the public) and tactical defeat, and the overlooked targets that could have had a greater long-term strategic effect (e.g., fuel storage and ship repair yards), set the strategic stage for the United States to enter the war, conduct full wartime mobilization and ultimately defeat the Axis powers. The country showed itself resilient to a localized kinetic attack as large as Pearl Harbor. The nation, with much hard work and sacrifice, ultimately achieved post-attack capabilities far beyond what it possessed pre-attack. A lesson of the “No More Pearl Harbor” analogies can be “Do not get caught unprepared and unaware.” What those analogies could also invoke are the memories of the other four (4) years of warfare that ended with enemies vanquished and America a dominant global super power. I am not asserting that a pervasive or prolonged contested cyber environment will lead to a victorious United States. I am suggesting that invoking “Pearl Harbor” to avoid surprise is a falling prey to the false analogy fallacy. Additional counter arguments to the analogy could include few people anticipated raids on Pearl Harbor, while watchers of daily news have heard stories of how easy it is for kids, hackers, criminals and nation-states to exploit our vulnerable IT systems and cause us harm. Clearly if a large scale cyber attack comes, no national or company leaders should reasonably claim the idea of such an attack had never occurred to them.

Another analogical appeal is comparing computer network defense to France's Maginot Line. The analogy frequently starts with the assertion that static computer network defense is as useless as the Maginot Line. The pre-World War II ([WWII](#)) Germans adapted to the presence of the Maginot Line with their decision to bypass the fortification zone—the 'Line' was a zone of defenses both laterally and in-depth, not simply a single line of defenses—in their May 1940 invasion of France. One of many military art and sciences lessons promulgated since 1940 is that static defense, with no ability to maneuver, surrenders the initiative to the offense—the attacking enemy. The attacking enemy can decide when and where to attack, while the defenders must defend their entire line at all times. A variant on this lesson is the perception that France placed all her war-delaying bets on the creation of a zone of defense impenetrable to expected attackers. With those bets, she deprived herself of defenses elsewhere. The lack of defenses along the French-Belgium border was what the Germans exploited—the Germans invaded France using a route through neutral Belgium. These analogies, with their abstractions and omissions of details, are repeated within the computer security world in the egg-defense model (aka the M&M model)—a hard shell and soft unprotected interior. The hard shell usually refers to defensive infrastructure facing exterior threats such as firewalls, ingress & egress filtering and monitoring, and border intrusion protection and defense systems ([IPS/IDS](#)). The soft interior usually refers to the perceived lack of defenses throughout the rest of an organizations' infrastructure and the portions perceived to have no direct contact with the outside world. These analogies are not wrong per se, but nor are they perfect fits in their choices of what to include and what to ignore or abstract. Indeed, examining each analogy shows points of comparison from which it is reasonably apropos to draw lessons learned. Examination also shows points of dissimilarity, some of which may be substantial enough to require yet another analogy, or other viewpoints.

Fundamentally, analogical reasoning is a useful tool in the human kit bag of reasoning skills. Ironically, if there is any cure to the problems of analogical reasoning—besides not using it at all—the cure lies in *more* analogical reasoning. Analogies, as conceptual models, deliberately abstract away details of their subject matter. The application of multiple analogies, each with their flavors of 'wrongness' can provoke the recognition that

there are few singular correct answers to extant problems—demonstrating George Box’s truism that “All models are wrong, but some are useful” (1979).

This section of the literature review is not intended to express an opinion that there are no effects in contested cyber environments. Nor am I opining that contested cyber environments will leave countries, companies, and people completely unaffected—the people of Estonia and Georgia were inconvenienced, scared, and forced to adapt. The psychological effects were present, well reported, and possibly worse than they might have been. Cyber enabled espionage can, and likely has, led to death and imprisonment of spies, protestors, opposition parties, as well as the relations of those people. Companies have lost competitive advantages through loss of intellectual property, suffered loss of trust through data breaches, and some may have gone bankrupt—clearly effecting the shareholders, employees, customers, and whatever supply chains of which they were members.

This portion of the review supports the notion that individuals, organizations, and governments need to spend more effort at making better estimates of ‘badness’ in contested cyber environments. It asserts that organizations, their leaders and workers, should not accept assertions that all contested cyber environments are inherently worse than other forms of risks to which they are accustomed, and to varying degrees, already resilient. Finally, the review puts forth evidence that short of survivability challenges, contested cyber environments are not as fundamentally different a mechanism driving adaptation as some choose to believe. Finally, a recurring theme in this section, as well as the entire dissertation is context matters as does nuance in interpretation and reaction.

Related literature corpus and assessment

Overview

The [Literature Review](#)’s [Introduction](#) highlighted multiple areas of related work. This section explains how I came to choose these sources from the corpus of texts, journals, and conferences I could have chosen.

When collecting sources and literature associated with resilience to contested cyber environments, it became evident there is a multidisciplinary aspect to the approaches taken by researchers. I cast a fairly wide net of search terms using Google™, Google Scholar™, and Web of Science™, using back-citation tracing, and adjusting search terms and patterns

while reviewing sources. I then input the data into the SNA software called [ORA™](#), from Carnegie Mellon University's ([CMU](#)) CASOS. ORA™ supports application of social and network science methods and techniques to the collected data. The collected data included the following: authors, titles, publishers, journal/source, year, hyperlinks to original articles, and links to similar articles (as offered by Google Scholar™). Collection of citations, sources, and books via these web sources lead to over 14,839 unique sources for which this section provides a review and analysis. Details of the search methodology are in the [Literature Review Bibliometrics](#) appendix starting on page [2-1](#).

Semantic analysis

Prior to using latent Dirichlet allocation ([LDA](#)) (Blei, Ng, & Jordan, 2003) and latent semantic analysis ([LSA](#)) (Laundauer, Foltz, & Laham, 1998) text analysis options in ORA™, my hypothesis was there would be links of varying strength between various aspects of resilience research. The hypothesized links, from intuitions based of 20 years as a computer scientist and over 10 years in the information assurance arena, are shown in [Figure 9](#). I also expected that there would be three dominate forms of M&S discussed in the research literature, depicted as turquoise ovals in the figure.

I expected there would be links between the HRO, general risk management and the business continuity communities. I presumed there would be links between the business continuity and disaster management communities as well as the cyber risk management and the general risk management clusters of authors and topics. I also assessed there would be links between the business continuity community and the organizational behavior and learning communities—after all, continuity of operations in the face of adversity is a learning experience if ever there was one! Finally, I had a hypothesized that there would be stronger and more numerous links between the cyber risk management community and the M&S community, than between M&S and the other groups. Within the M&S field, I expected to find three main families of stochastic simulations: agent based, system dynamics, and discrete event. I also expected that the generalized cluster of M&S would contain many of the same references that serve as the foundational pillars of modeling and simulations.

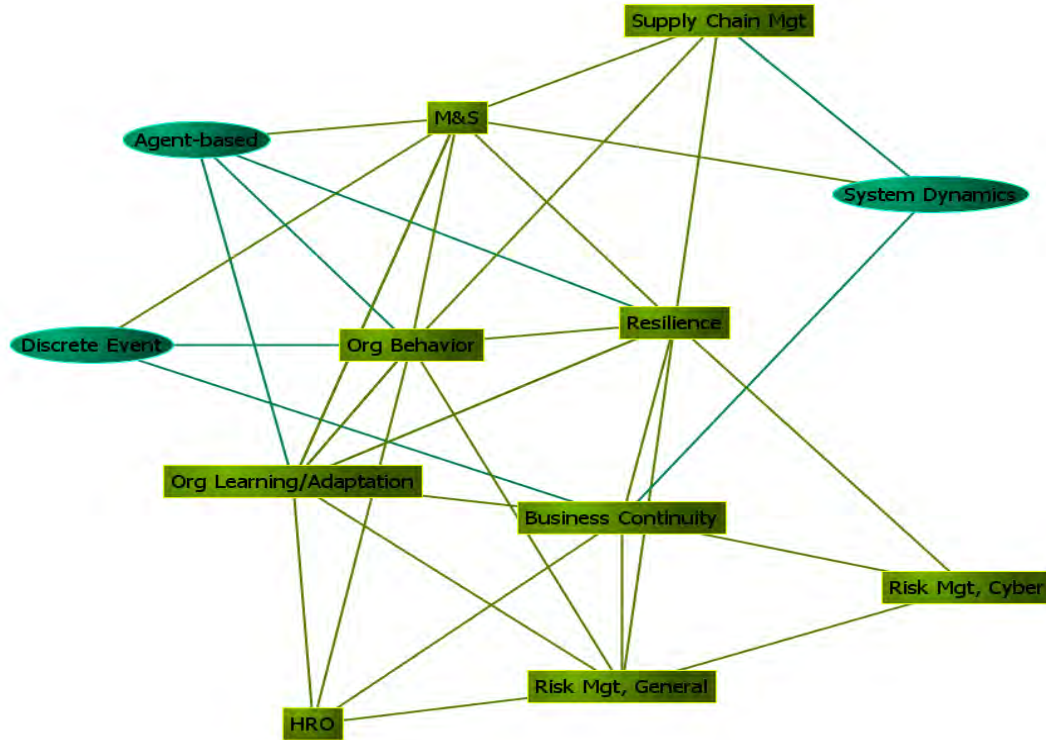


Figure 9: Intuition based clustering and links between clusters of the Literature Corpus

The descriptive statistics for the collected citations and their respective meta-data are in [Table 6](#).

This review is not a review of 14,800+ articles' concepts. The section is a demonstration using various network analytics that there are both links between various research communities and the absence of links that should reasonably exist through shared and common interests. Though [LSA](#) and [LDA](#) both require a researcher to assert, *a priori*, the number of clusters to which the algorithm should apply, I did not have strong evidence that [Figure 9](#) was accurate. I created the figure using intuitions from 20 years exposure to the fields of computer science, computer engineering, risk management, information and computer security, operations planning and contingency planning. As such, I ran LSA using ORA™ for topic counts that ranged from 3 to 11, inclusive. I did the same for LDA using 5,000 iterations, a step size of 100, and $\beta=0.01$.

Table 6: Descriptive statistics of citations collected for literature review

Total Number of articles	14,838
Number of books⁸	796
Number of ‘citations’⁹	1,091
Authors	19,750
Concepts	4,276
Journals	5,013
Publishers	755
Schools	272
Websites	743
Years	43
Networks	53
Links	15,635,378
Total Density	0.75%

LSA (see also [Figure 10](#) through [Figure 15](#)) was able to generate meaningful fully connected graphs with starting with 6 topics. The 6 topic LSA graph ([Figure 10](#)) depicts a fully connected graph though the intra topic links as well as the inter-top links are generally weak links. The 7 topic LSA graph ([Figure 11](#)) is also fully connected though the far left topic is only weakly connected to the remainder of the graph through a single shared node—“risk_assessment.” This graph however

does reveal stronger intra topic links. The remaining topics have multiple inter topic links indicating shared concepts between topics. Of note is the topic of “simulation” does not occur using LSA until the number of topics rises to 10—indicating that [Figure 9](#) is overly optimistic in establishing strong links between other key words. This lack of such a central topic for this dissertation is one indicator that the dissertation is providing an additional link between research topics.

⁸ Generally identified within Google Scholar with the [B] or [BOOK] prefix in front of titles, as well as texts encountered by the author during readings and included in the search criteria as deliberate inclusion items

⁹ Generally identified within Google Scholar with the [C] or [CITATION] prefix in front of scholars, or citations pulled from web sites such as citeseer.org. These entries also do not generally have a readily accessible copy of the original source material available via the internet.

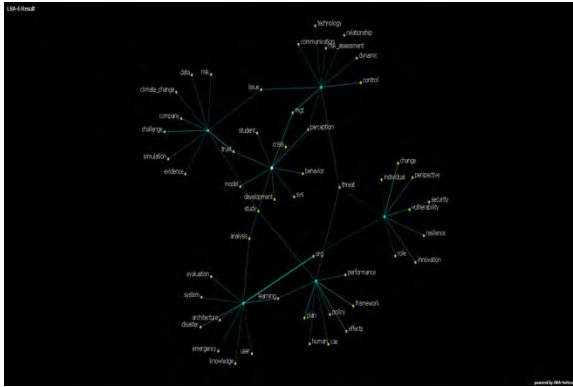


Figure 10: LSA 6 topics, top 10 members/topic

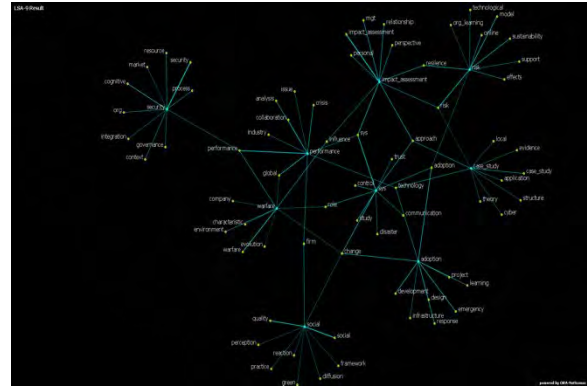


Figure 13: LSA 9 topics, top 10 members/topic

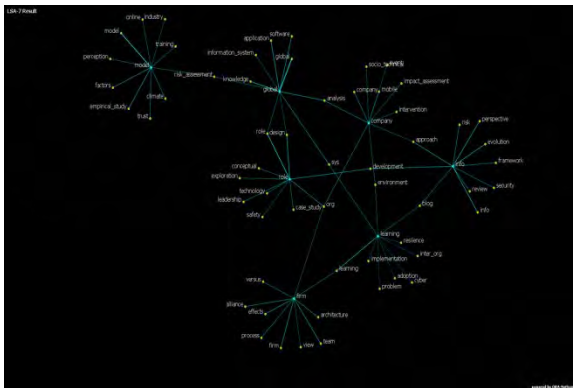


Figure 11: LSA 7 topics, top 10 members/topic



Figure 14: LSA 10 topics, top 10 members/topic

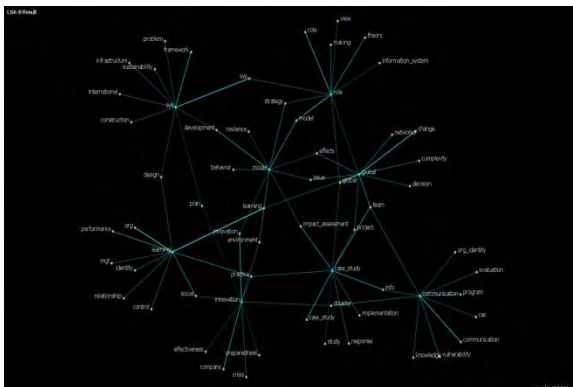


Figure 12: LSA 8 topics, top 10 members/topic

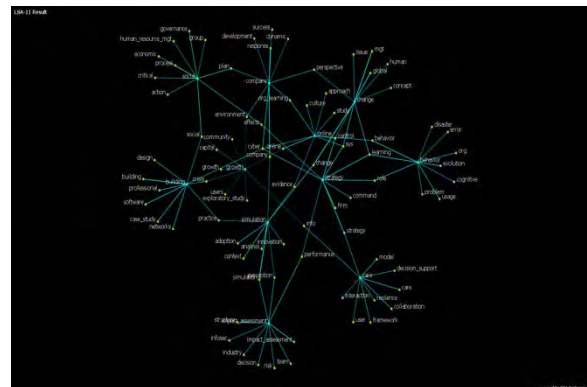


Figure 15: LSA 11 topics, top 10 members/topic

Since the 10 members per topic LSA groupings are the first to incorporate this key aspect of the dissertation ([M&S](#)), it is appropriate to conduct a comparison with the graphic shown in [Figure 16](#) to the topic-connections shown in [Figure 9](#). Within [Figure 16](#), the light blue nodes are the topics (labeled with the concept with the highest value) and the yellow nodes are the highest valued concepts that the [LSA](#) algorithm found when performing single value decomposition ([SVD](#)) on the concept x document matrix. The links' colors vary by value (red highest, blue lowest, with even distribution of color assignment) and the link value scales the link width.

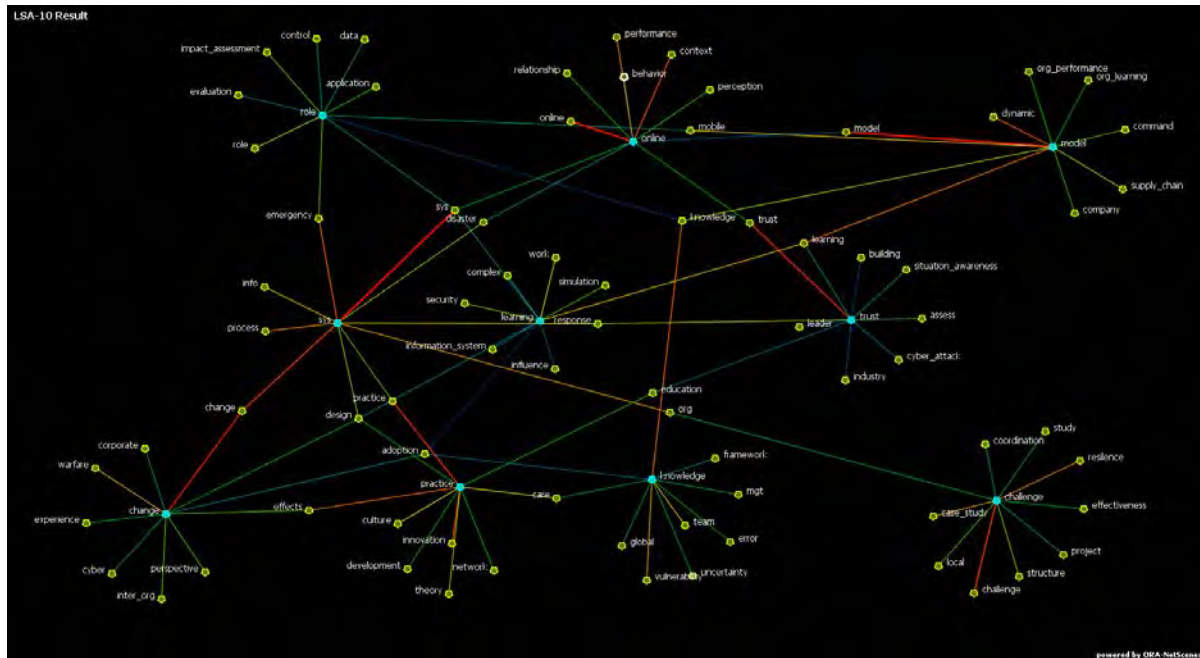


Figure 16: ORA™ generated LSA analysis of collected citations with 10 topics.

This depiction of automated analysis compares somewhat favorably to the intuition depicted in [Figure 9](#) for some clusters as well as some of the inter-cluster links. Supply-chains and the management of supply chain risk appear to align with the upper right topic of “model” while overlapping organizational learning. Modeling and Simulation does not appear as its own topic, but is a related node to the “response” topic in the center of the figure that also overlaps with organizational learning, but does not otherwise link any of the other topics—the cause of which remains unexplored. The originally expected notion of resilience appears in the “challenge” topic at the lower right. Related words of “case study” as well as the absence of any first or second order links to simulation are reflective of the room for improvement in the use of simulation in studying and assessing resilience. High Reliability Organizations, as sociotechnical systems appears to align with the LSA topic of “sys” (short for system) center-left of the figure. The associated terms disaster, emergency, and process lend credence to that alignment as well. The “Knowledge” topic, bottom center-right, aligns with the originally expected concept of generalized risk management while the “change” topic, bottom left, aligns with the cyber risk management. The originally expected organizational learning also appears to align itself with the LSA derived “practice” concept, though like the literature itself, the learning appears to be more market oriented than cyber event preparedness.

[Figure 16](#) depicts graphically that there is indeed a gap between the research about organizational resilience (how organizations learn and adapt to adverse events) and research into cyber risk management. Until researchers begin to bridge these and other gaps, there is significant opportunity for duplicated work, missed findings, and other research inefficiencies. There is also room for better integrating general risk management research with resilience research and organization learning—the fit seems natural, and its conspicuous absence should serve as the basis for calls for broad agency announcements or requests for proposals.

[LDA](#) (see also [Figure 17](#) through [Figure 22](#)) was unable to generate fully connected graphs until 13 topics. The 8 topic to 12 topic applications of the LDA algorithm generated graphs with 2, 3, or more components. Since the 13 topic LDA iteration was the first to generate a fully connected graph, a comparison with the intuition-based graphic shown in [Figure 9](#) is appropriate. Like [Figure 16](#), within [Figure 22](#) the light blue nodes are the topics (labeled with the concept with the highest value) and the yellow nodes are the highest valued concepts that the LDA algorithm found when executing. The links' colors vary by value (red highest, blue lowest, with even distribution of color assignment) and the link value scales the link width.

The upper left topic, labeled “cyber” is likely generated from the number of sources discussing the future of warfare augmented with cyber warfare. I had not included a “cyber war” node in the expected model, as it seemed a degenerate inclusion. The center-top topic of “worldwide” aligns, with overlaps, the expected organizational behavior node. The “adaptation” node on the right-center of the figure aligns, especially when combined with its neighbor “info,” to the notion of organizational learning and adaptation. Of interest is the lack of direct link between these two nodes and the node in the center-bottom labeled “resilience.” This lack again indicates a gap between the resilience research and organizational adaptation and learning fields. There is a weak link between the “resilience” node and the system node on the left-center of the figure, also indicating a weak link between simulations and resilience areas of study.



Figure 17: LDA 8 topics, top 10 members/topic

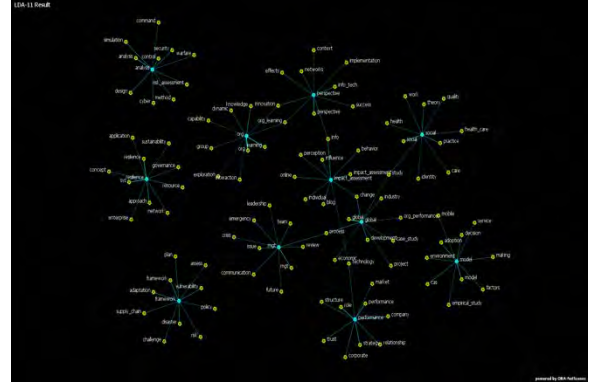


Figure 20: LDA 11 topics, top 10 members/topic



Figure 18: LDA 9 topics, top 10 members/topic

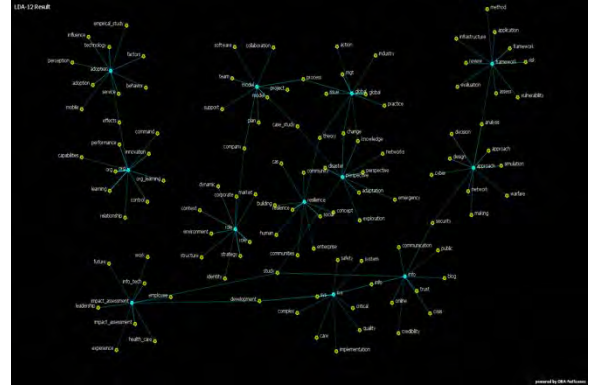


Figure 21: LDA 12 topics, top 10 members/topic

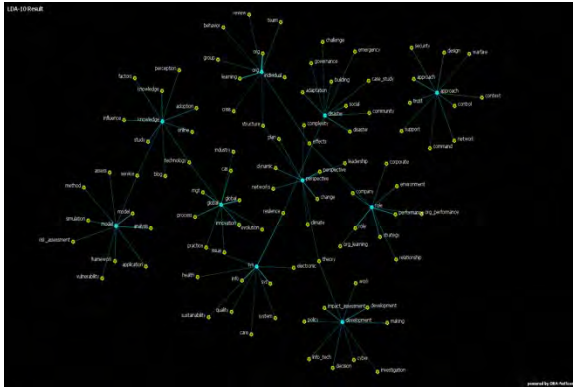


Figure 19: LDA 10 topics, top 10 members/topic

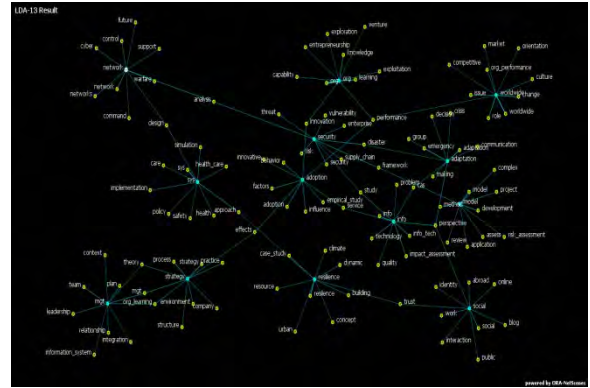
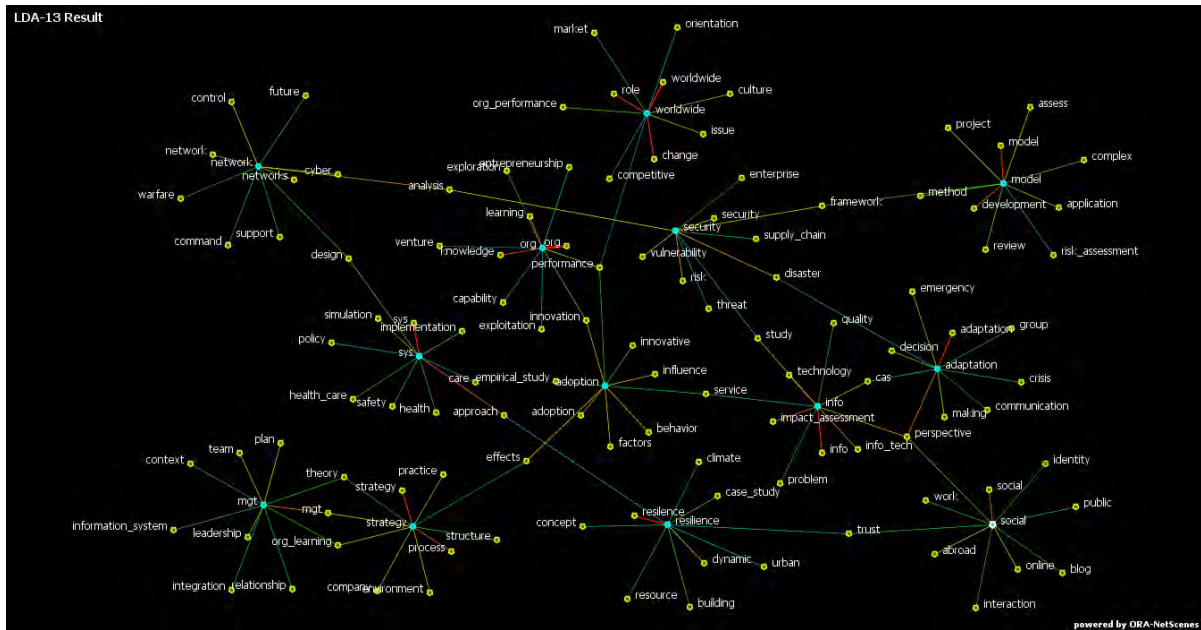


Figure 22: LDA 13 topics, top 10 members/topic



Network Analysis

ORA™ uses network analytics to help analysts identify Key Entities. Depending on the nature of the underlying quantity and nature of the underlying data, analysts can attain a higher confidence that their interpretations of the data attain at least face validity. With face validity, they can then use multiple forms of analysis to triangulate results and gain further confidence.

Key Entities

ORA™'s Key Entity functionality is unique across the various forms of social network analysis software and tools. The Key Entity functionality uses as many of the 170+ measures in ORA™'s repertoire, as the underlying data can support. For each measure, ORA™ stores a user-specified number of nodes (the default is 3) with the highest calculated values. For each set of measures applicable to the various node types (e.g., measures applicable to agents) in the data set, ORA™ then calculates the percentage frequency each of those high-value nodes appear in each measure. The ORA™ report then displays the number of nodes the user specified from the list of nodes' with calculated values. The advantage to this approach is that individual measures may correlate with each other or have high inter-measure variability (Borgatti, Carley, & Krackhardt, 2006; Kathleen M. Carley, 2002d; Frantz & Carley, 2005). However, when nodes are consistently in the top-place ranks

aggregated across multiple measures, analysts can reasonably have more confidence in the relevance of those nodes to their questions of interest.

In set notation, Key Entities reports in ORATM follow the steps below. Equations (3) and (4) define the nodes and edges respectively. Equation (5) defines the set of possible measures applicable to the available nodes and edge.

$$\mathbb{N} = \{ \text{node} \} = \{ n_1, n_2, \dots, n_{|\mathbb{N}|} \} \quad (3)$$

Equation 3: Node set definition in set notation

$$\mathbb{E} = \{ \text{edges} \} \mid \text{edge}_{n_i} \subseteq \mathbb{E} \wedge \text{edges}_{n_i} = \{ \{n_1, *\}, \{*, n_1\} \} \quad (4)$$

Equation 4: Edge set definition in set notation

$$\mathbb{M} = \{ \text{measure}(\mathbb{N}, \mathbb{E}) \} \mid \text{measure}(\mathbb{N}, \mathbb{E}) \neq \emptyset \quad (5)$$

Equation 5: Measures set definition in set notation

Each node-level measure (as distinguished from a network-level measure that generates a single value) generates a set of real values where each value's place in the set corresponds to the place in the node set of the node being assessed as shown in (6). In other words, a real value b_1 in (6) corresponds to a value calculated using node n_1 in (3).

$$\forall m \in \mathbb{M}, m = \{ \mathfrak{R} \} = \{ b_1, b_2, \dots, b_{|\mathbb{N}|} \} \mid b_i = m(n_i, \text{edges}_{n_i}) \quad (6)$$

Equation 6: A measure's output definition in set notation

For the measure m calculated in (6), the top x calculated values are retained, realizing that each of those values represent the node from which it was calculated. This retention of the top x values is shown in (7) for any arbitrary measure m as is the mapping from real value b_1 to node₁. The set of nodes corresponding to the top x calculated values is shown in (8).

$$\mathbb{X} = \max_{1..x}(m) = \left\{ \forall x, \max_x(b_1, b_2, \dots, b_{|\mathbb{N}|}) \right\} \mid b_i \rightarrow n_i \quad (7)$$

Equation 7: A set of maximum values from a measure's output in set notation

$$\mathbb{Y} = \{ n_a, n_b, \dots, n_x \} \quad (8)$$

Equation 8: A set of node identifiers corresponding to maximum values from a single measure in set notation

Across all relevant measures, the algorithm builds a set of top rank nodes as shown in (9). The algorithm then builds a set of values using every node in the graph. It counts the number of times each node in \mathbb{N} appears in the set \mathbb{Z} , divides by the number of measures and achieves the percentage of measures the node has achieved a top ranked value. This set of

values is shown in (10). Finally the algorithm takes the top x values from \mathbb{T} , relates them back to their contributing node identifier, and presents the identifiers to the analyst as shown in (12).

$$\mathbb{Z} = \{Y_m, \forall m \in \mathbb{M}\} \quad (9)$$

Equation 9: A set of measures' results as sets of node identifiers in set notation

$$\mathbb{T} = \forall n \in \mathbb{N}, \frac{\sum_m \begin{pmatrix} 1 & n \in Y_m \\ 0 & \text{otherwise} \end{pmatrix}}{|\mathbb{M}|} \quad (10)$$

Equation 10: Calculating the frequency of occurrence a node is in the maximum value set of all relevant measures

$$\mathbb{KE}_{freq} = \max_{1..x} (Y) = \{\forall x, \max_x (T_1, T_2, \dots, T_x)\} | T_i \rightarrow n_i \quad (11)$$

Equation 11: A set of maximum frequency of occurrence values in set notation

$$\mathbb{KE} = \{ke_1, ke_2, \dots, ke_x\} \quad (12)$$

Equation 12: A set of node identifiers corresponding to maximum frequency of occurrence values in set notation

When performing this function across the data collected for the corpus of citations, ORA™ helps identify the following key entities. The figures below offer another way to visualize the key entities describe by the equations above. In particular and of note, there are no dominant (i.e., an author or Journal or other entity that reaches higher than fifty percent (50%) across all the various applicable measures. This result reinforces the perception that there is significant room for research, Journals, and publishers to increase their cross-discipline research as well as apply and absorb completed research from outside their primary areas of focus.

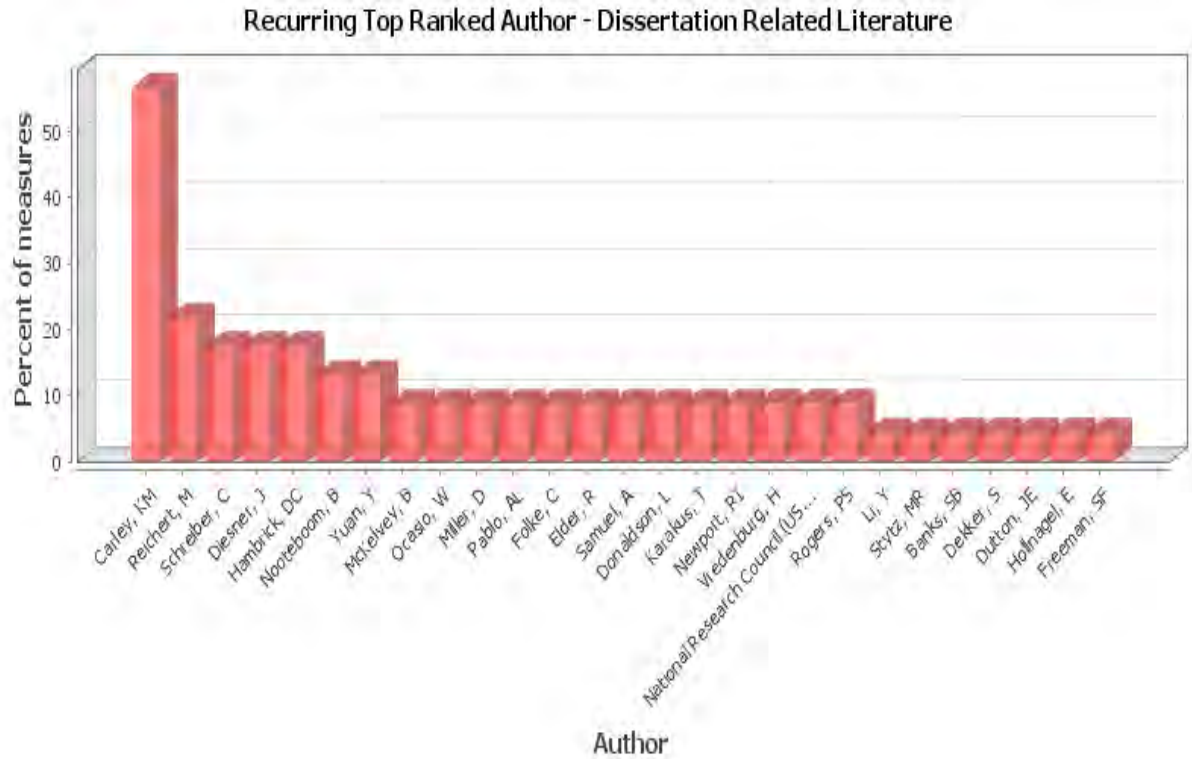


Figure 24: Key entity 'Author'

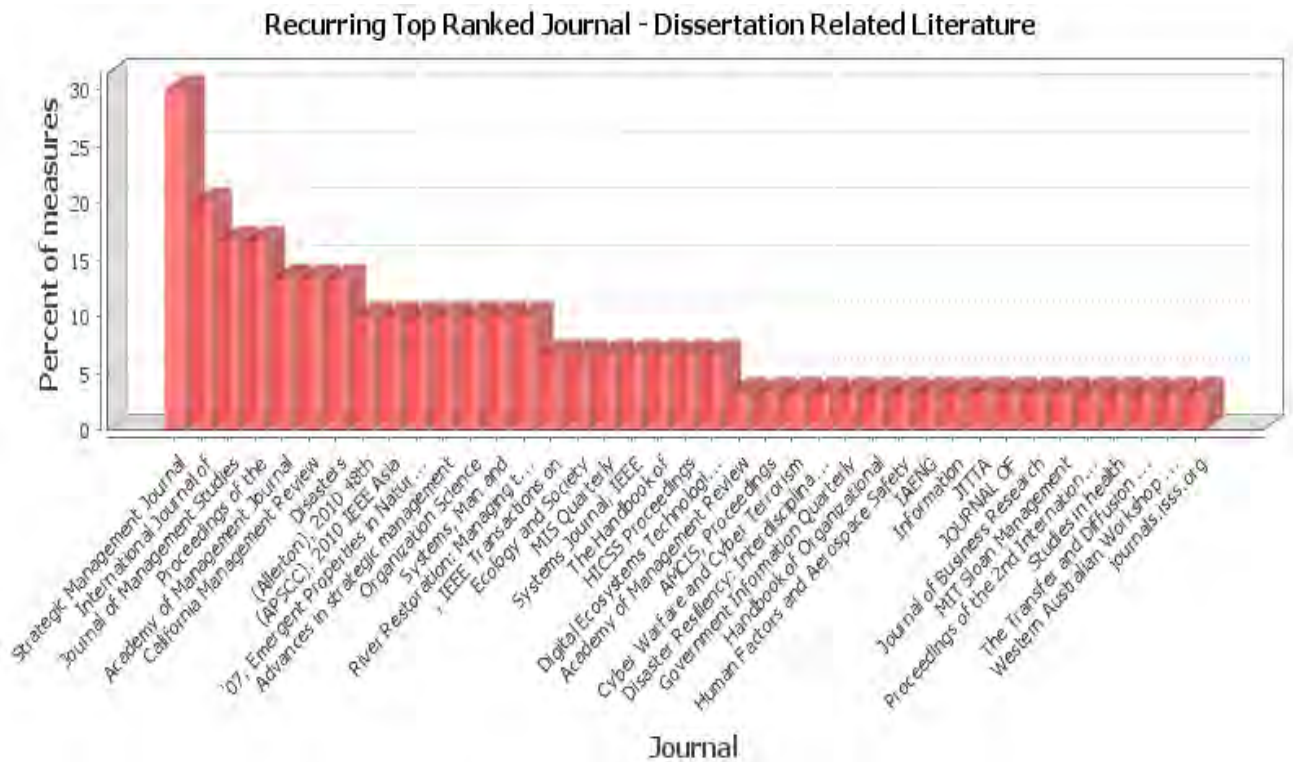


Figure 25: Key entity 'Journal'

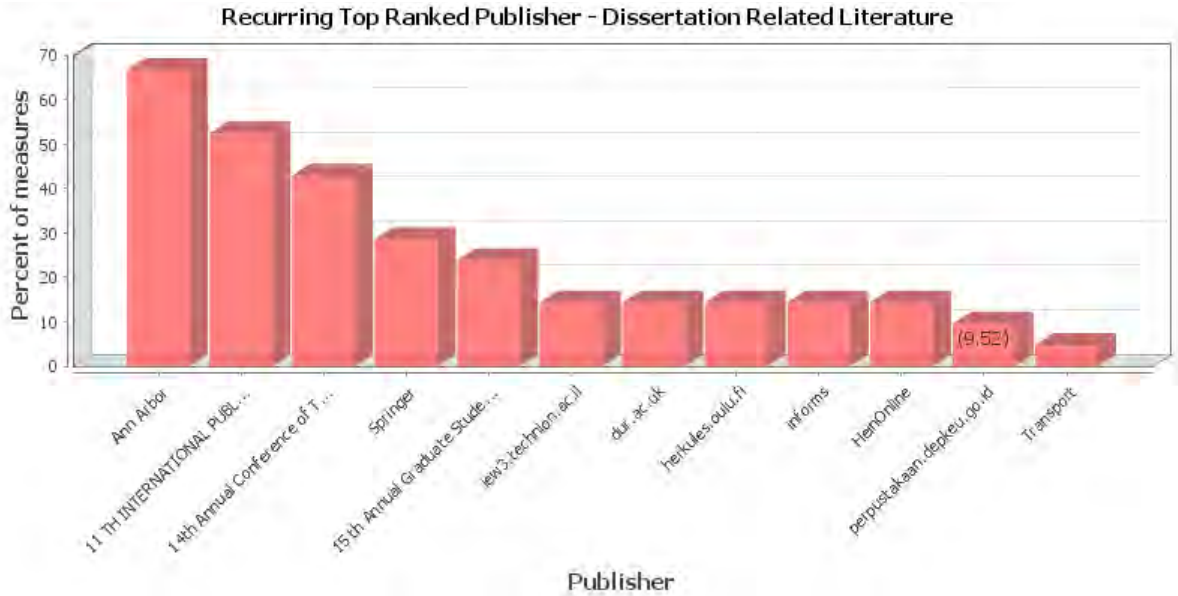


Figure 26: Key entity 'Publisher'

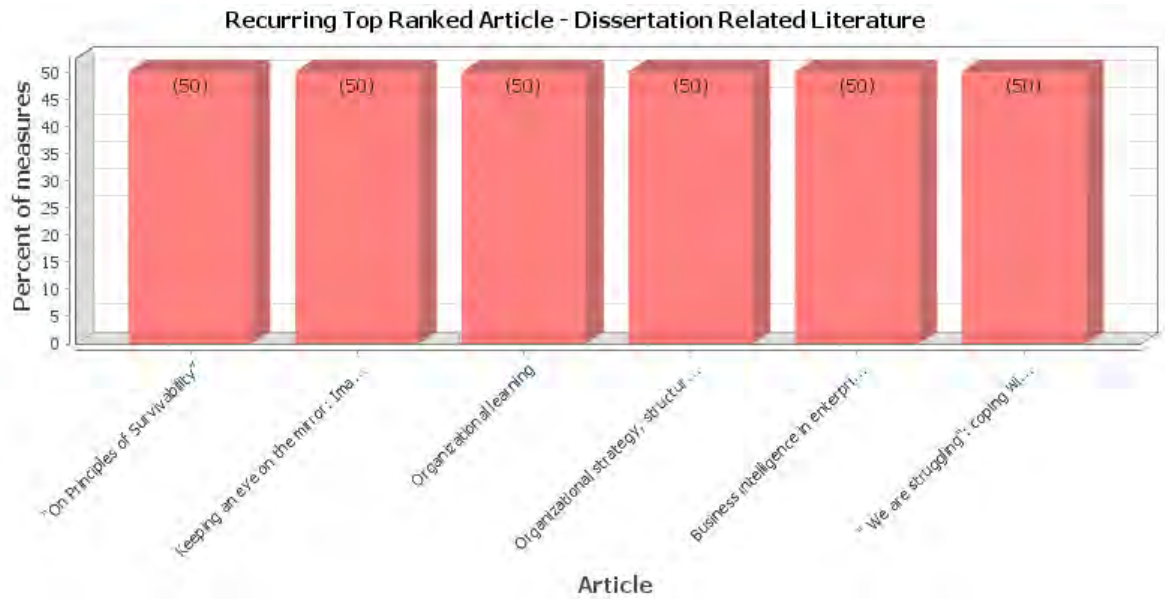


Figure 27: Key entity 'Article'

Co-Authorship Networks

The full visualization of the co-authorship network (i.e., the graph such that an edge between two author nodes indicates a shared authorship and the weight of the edge indicating the number of distinct co-authorship efforts) is a undifferentiated ball of nodes and edges with the vast majority of nodes involved in dyads or triads with edge weights of one (1). However, when I added a progressively higher filter on the edge weights that hide all edges below the filter threshold, the graph rapidly degenerates into very small clusters of authors who write with each other. At filter weight of less than 2 (see [Figure 29](#)) there are a small

number of such clusters that form author-strings or more traditional core-periphery networks. With the filter set to hide edges with less than a weight of 3.5 and hiding isolates, a disconnected graph remains (see [Figure 29](#) for the unzoomed view, and [Figure 30](#) for the zoomed in view) making it easier to see that very few cross-domain co-authorship efforts exist in the realm of organizational reliance to adverse cyber environments. When I added pendant nodes back into the graphs, the co-authorship networks remain unconnected (as expected) except for clusters of prolific authors, as shown in [Figure 31](#). Adding the pendants into the graph depicts the increased opportunity for collaboration by adding related authors.

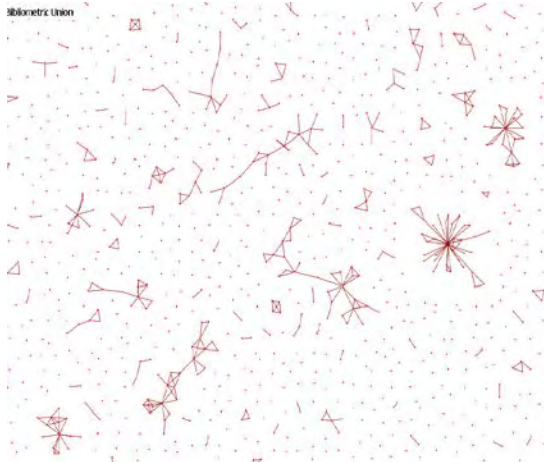


Figure 28: Zoomed in co-authorship network, edges with weight < 2 hidden, zoomed in on prolific author clusters

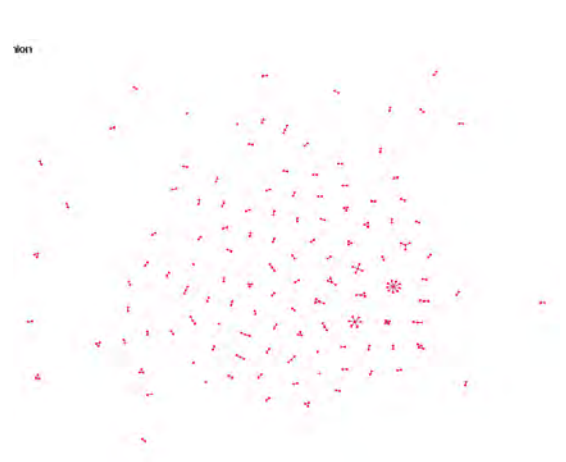


Figure 29: co-authorship network, edges with weight < 3.5 hidden, pendants removed, not zoomed in

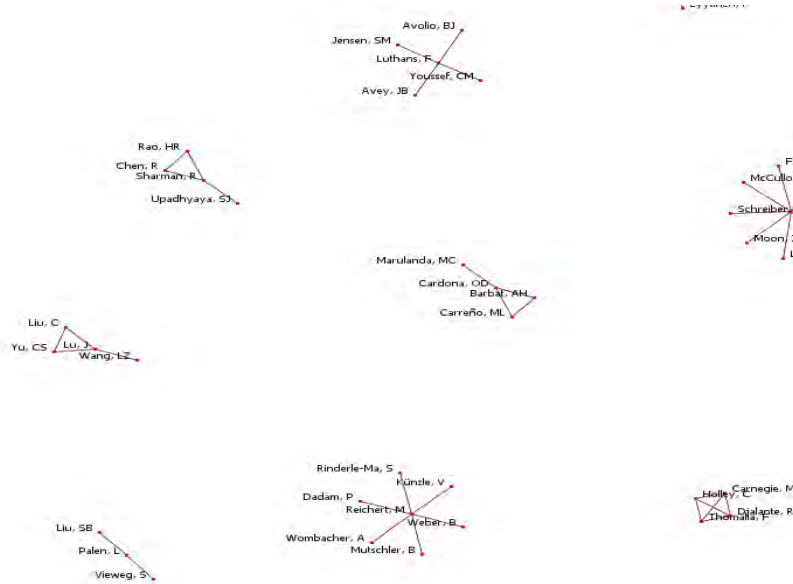


Figure 30: Zoomed in co-authorship network, edges with weight < 3.5 hidden, with pendants removed, zoomed in on prolific authors

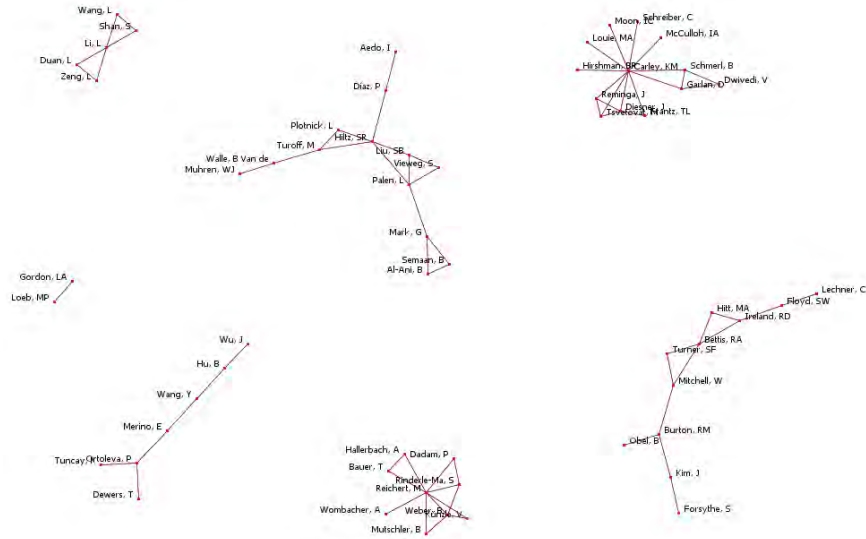


Figure 31: Zoomed in co-authorship network, edges with weight < 3.5 hidden, with pendants remaining,, zoomed in on prolific authors

Co-Citation Networks

The full visualization of the Co-Citation network (i.e., the graph such that an edge between two article nodes indicates a shared citation and the weight of the edge indicating the number of distinct shared citations) is more akin to a head of cauliflower (see [Figure 32](#)) than an undifferentiated ball of nodes and edges. There are clearly distinct clusters of well-cited articles surrounded by increasingly less sparse connections between shared article citations. The co-citation network for books and articles (see [Figure 33](#) on the next page) shows a much less connected collection of co-citations between articles and books with the vast majority of nodes involved in dyads or triads with link weights of one (1).

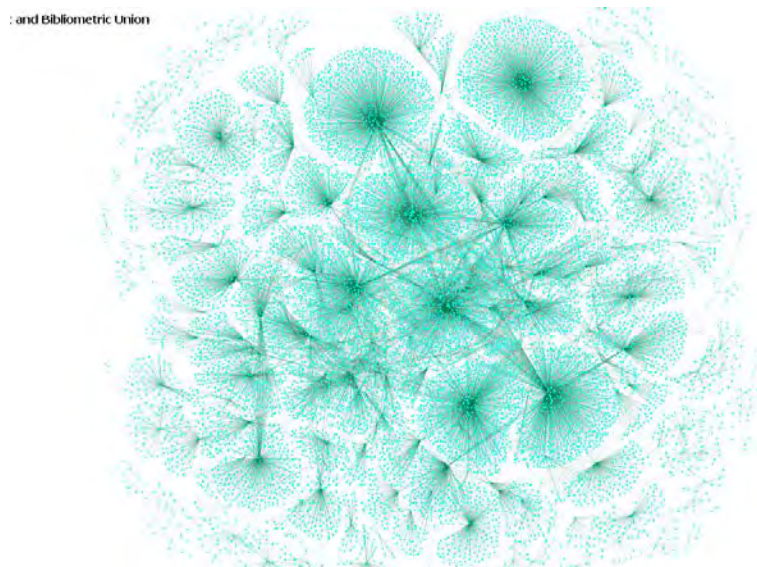


Figure 32: Co-citation network of article x article, no filtering

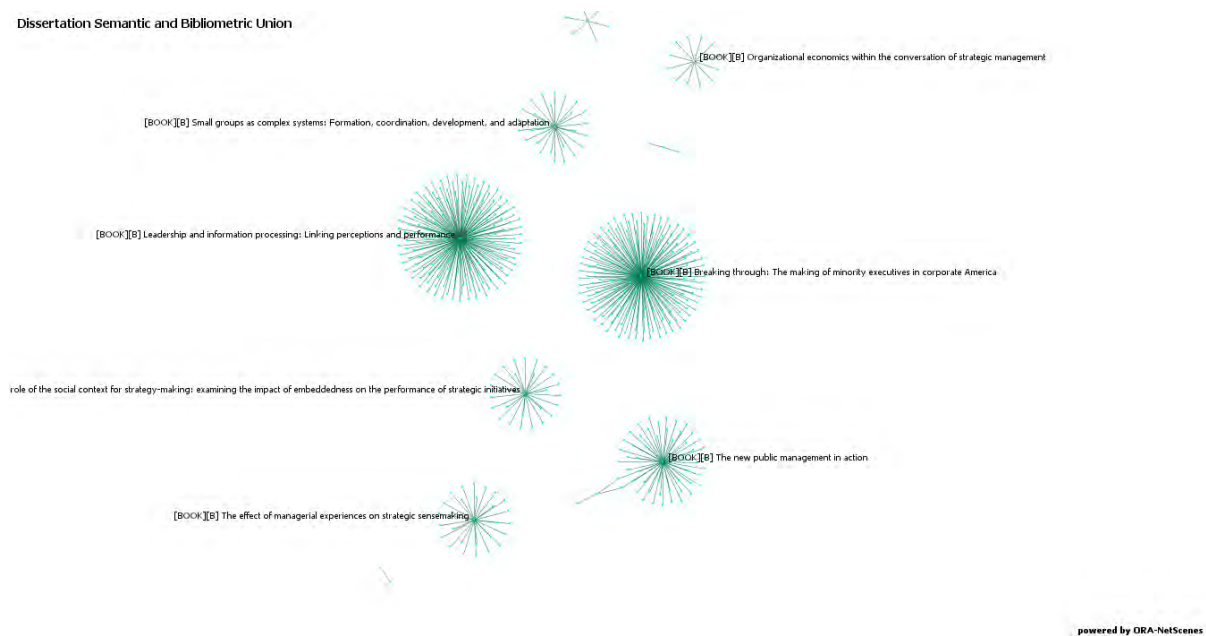


Figure 33: Co-citation network of article x book, no filtering

This [Overview](#) has presented bibliometric and textual analysis views of the related literature supplemented with visual renderings and graphs of the information. While useful, particularly to depict areas of overlap and under lap, these views need additional supporting evidence via explication and discussion of specific trends, texts and authors. The remainder of this section provides a review of literature from each of the clusters identified above.

Risk management

As noted in the beginning of the section [Why resilience? Isn't risk management enough?](#), traditional risk management starts with the idea of risk avoidance (K. D. Miller, 1992). There are other traditional tools of risk management besides avoidance with common ones being: prevention and reduction, retention, and transfer (Akintoye & MacLeod, 1997; Al-Bahar & Crandall, 1990).

An organization can avoid a risk if that is a feasible course of action; if there is a risk a rocket will blow up during launch, the organization could choose not to launch the rocket, much less attempt to build a rocket. If the organization's mission is to launch rockets, clearly this is an infeasible choice. Organizations whose missions are supported by cyberspace capabilities may decide it is equally infeasible to abandon the use of those capabilities in pursuit of their own requirements.

If an organization can reduce the *probability of occurrence* or the *impact* term in [Equation 1](#): (on page [24](#)) to near zero, the organization could drive the overall risk to near zero. To continue the rocket launching analogy, the organization may reduce the probability of an explosion through rigorous testing of systems and subsystems throughout their performance envelopes prior to an actual launch. For cyberspace-enabled organizations, they can reduce probabilities of certain types of event occurrences (e.g., catastrophic engine malfunction, hard disk failures and loss of data) despite being unable to reduce all events' probabilities to zero. Similarly, if the *impact* term drops to near zero, there is a greatly reduced requirement to reduce the *probability of occurrence* to near zero—as the impacts are negligible. For the rocket-launching organization, they may be able to reduce the impact of a launch vehicle explosion by having some sort of payload evacuation mechanism such that only the launch vehicle suffers the impacts—akin to the crew escape system on the Saturn V. For a cyberspace enabled organization, having fail-over systems and fail-over processes in place may make the impact on primary systems negligible.

Prevention and reduction are close cousins to avoidance. How much prevention and reduction an organization should pursue with respect to reducing risk from contested cyber environments is a question with as many answers as there are variations in organizational situations. Significant effort has gone into creating and publishing cyber risk management frameworks. Contributors to the field have been standards bodies (NIST, 2012), Federally Funded Research and Development Corporation ([FFRDC](#)) such as MITRE (MITRE, 2012c) and Software Engineering Institute ([SEI](#)) (Alberts & Dorofee, 2010) as well as individual researchers (Hoo, 2000; Pfleeger, Predd, Hunker, & Bulford, 2010; Ralston, Graham, & Hieb, 2007). Many of these frameworks offer extensions of the basic models of [Equation 1](#): and [Equation 2](#):

Some risk management frameworks involve a cycle of identification of possible threats and the vulnerabilities of organizations' assets to those threats, identification and implementation of mitigation measures, and a calculation of residual risks (Hoo, 2000; NIST, 2012; Wallner, 2008). Each of these has a component of the cycle that requires an organization to reduce one or more terms in the respective equations through implementation of one or more controls—measures put in place by the organization to cause a reduction in equations' terms. These risk-mitigation phases of the various frameworks' cycles help reduce the original level(s) of risk to level(s) that decision makers are willing to accept. Researchers and security practitioners often

refer to this acceptance of risk after efforts of reducing it as the acceptance of residual risk. Of course, this comfort level is subject to the usual limits of human decision heuristics: 1) representativeness, 2) availability of instances or scenarios, and 3) adjustment from anchor (Tversky & Kahneman, 1974). It also is important to recall that the extensions are cycles, and are not supposed to be a one-off execution of the process but a periodic, if not continuous exercise (Siegel, Sagalow, & Serritella, 2002).

Retention may often be a more practical form of risk management than the other three tools, as well as the fundamental last active step of a risk management process. An example of risk retention is the fact that the US Government retains the risk of loss of physical assets such as buildings, equipment, and other tangible items ("48 CFR Parts 202, 203, 211, et al.," 2011; USHR, 2012). The USG does not purchase insurance as a protection mechanism. There are undoubtedly many reasons for this governmental lack of transfer, but difficulties with enumerating the number of physical assets that embody the cyber and IT infrastructure (such as those experienced with the Navy/Marine Corps Intranet ([NMCI](#)) (Musich, 2001)), the states of repair, and precautions against loss or damage surely contribute to the challenge. I found no evidence of efforts to study whether the US government could sufficiently inform an insurance company of the types and quantities of cyber assets the government owns and operates; presumably the probability it could do so is small.

Risk transfer is a time-honored form of risk management by which the risk becomes a commoditized item: there are sellers and buyers of risk, with each side of the transaction attempting to reduce losses. The various insurance industries that exist around the globe are in the business of selling protection from downside risk, while charging their customers enough to cover losses and make profits. Cyber risk transfer markets are beginning to develop with supporting research (Bandyopadhyay, Mookerjee, & Rao, 2009; Böhme, 2005; Böhme & Kataria, 2006) at the consumer level and at the corporate level (D. R. Cohen & Anderson, 2000)—though a Chubb Group of Insurance Companies survey found 65 percent of companies forgo cyber risk transfer (Chubb Group of Insurance Companies, 2012).

Of these four tools, risk transfer and the acceptance of residual risk come closest to explicitly acknowledging that risk is not zero, and that there is nonzero probability of negative events occurring. Being able to rehearse for and adapt to those negative events is not explicitly

part of the tools for cyber risk management, as such rehearsals and adaptations frequently occur outside the areas of expertise of the cyber subject matter experts ([SMEs](#)).

Risk management frameworks

Risk management frameworks develop a common language for practitioners of risk management. Many frameworks have names or identifiers published by standards organizations such as Institute Organization of Standards ([ISO](#)) 31000 *A Structured Approach to Enterprise Risk Management* ([ERM](#)), NIST Special Publication 800-30 (Stoneburner et al., 2002) or SEI's Enterprise Risk Management Integrated Framework (Alberts & Dorofee, 2010). Some of these are deliberately general and do not explicitly reference cyber risk management, while others are very specific about including IT and cyber in risk management planning, such as the DoD Directive (DODD) 8500.01E *Information Assurance* (Department of Defense, 2007) and Chairman of the Joint Chiefs of Staff Instruction ([CJCSI](#)) 6510.01F *Information Assurance and Support to Computer Network Defense* (Joint Staff J6, 2011).

Miller (1992) also developed a comprehensive risk management framework specifically for international companies which are using information technology to enable their operations. Despite this use of IT, the primary references to technology in Miller's framework seem to relate to whether competitors will produce a technical innovation in products or processes, not how the organization adapts to degradation of its IT capabilities.

The frameworks above, and others I am aware of, implicitly treat change in the operating environment as a nearly ever-present phenomenon. The implicitness is communicated in the admonishments to risk-managers and organization leaders to treat risk management as a never-ending cycle of activities. However, the lack of explicit planning and rehearsing for low-probability negative events reduces the efficacy of these frameworks in establishing mission assurance. Another drawback to frameworks, despite the as-designed cyclic nature, is the data supporting assessment with compliance to the framework tends to be snap-shot in time data, not a continuous data stream or constant assessment. This lack of continuous assessment means that compliance to framework requirements are lagging indicators of risk reduction where the lag could be days to weeks and sometimes longer. This lag between data collection and transformation to information also reduces the confidence in mission assurance assessments.

High Reliability Organizations (HROs)

What makes [HROs](#) fundamentally different from learn-through-experience/experimentation organizations —those able and willing to learn from errors with less than existential consequence (La Porte & Consolini, 1991)? Early research of HROs used examples of high-costs-of-failure operations such as US Navy aircraft carrier flight deck operations and Federal Aviation Authority ([FAA](#)) control tower operations as motivating examples (La Porte & Consolini, 1991; Roberts, 1989). Two characterizations from (Roberts, Rousseau, & La Porte, 1993) encapsulate those difference: (1) HROs tend to focus on process reliability because outcomes are impossible to achieve without the process—carrier flight deck operations would be an exemplar; (2) HROs tend to have expectations of high-tempo for sustained periods of time while maintaining their ability to do so—air traffic control being a prime exemplar. Research into HROs over the last thirty years has flourished, extending into fields as diverse as medical practice (Ash, Berg, & Coiera, 2004; Baker, Day, & Salas, 2006), and disaster and emergency planning (Crichton et al., 2009; Lally, 2013) as well as post facto explorations as to event causation (e.g., Shrivastava’s book on Bhopal (1987) as well as post space shuttle *Challenger* research (Kathleen M. Carley, 1991)).

One of the more interesting, though difficult to model, aspects of HROs is the multiple forms of self-organization they take on. Structures that correspond to routine operations differ from those in peak-loading conditions, which in turn differ from in extremis conditions (Roberts, 1989, 1990). Unfortunately, for organizations that do not perceive themselves as operating in these conditions, there appears to be less willingness to transform successful HRO practices than might be fruitful. Though the specific organizations in this dissertation are not HROs, the ability of agents in the simulation of this dissertation to not be restricted to a single form of organizational structure can represent this simultaneous structuration seen with HROs.

Supply Chain Management and Resilience

Supply Chain Management ([SCM](#)) is a field that enjoys a rich history dating to the early 1980s (Cooper, Lambert, & Pagh, 1997). A founding idea behind SCM was the interorganizational control of costs associated with inventory (Cooper et al., 1997; Min & Zhou, 2002). The International Center for Competitive Excellence defined SCM as “the integration of business processes from end user through original suppliers that provides products, services and

information that add value for customers” (Cooper et al., 1997). Implicit in this definition, and its surrounding literature, is the need to control, mitigate, and adapt to the risks faced by companies with supply chains. Though Cooper et al.’s literature review reveals differing opinions of scope, she points out that there is widespread agreement about the need for information systems integration, planning and control activities. Indeed, of the seven authors she presents comparing/contrasting SCM and business process reengineering perspectives (Houlihan, Stevens, Cooper and Ellram, Hammer & Champy, Andrews and Stalic, Hewitt, and Towers), all consider IT structure supporting information flow a critical component of their research and business practices (Cooper et al., 1997). Yet the notion of resilience, of ensuring these optimized and efficient systems can adapt to unexpected environments is present only by implication, suggesting a gap in awareness of the need to balance optimality and efficiency (Gunderson, 2003; D. D. Woods & Branlat, 2011).

One of the principal tools of exploration in this field is empirical study. One popular alternative to empirical study is computerized [M&S](#) (Swaminathan, Smith, & Sadeh, 1998). Min and Zhou’s review of M&S of SCM divides the various forms of M&S into four categories; the traditional deterministic and stochastic models, a hybrid model of the two, and IT-driven (2002). The use of IT-driven models (e.g., near-real time monitoring of various stages in the chain, as well as near-real-time adjustments to process) also exposes SCM practitioners to risks, in particular the triad of confidentiality, integrity, and availability (G. E. Smith et al., 2007). For supply chains that use IT to drive or enable specialization versus generalization, any event that creates effects within the CIA triad puts those chains at risk of imbalance (D. D. Woods & Branlat, 2011).

Reductions in costs, improvements in customer service, faster speed to market, and more efficient use of resources are all measurable by-products of the exploitation of robust cyber environments (G. E. Smith et al., 2007). Given these documented benefits, how do SCM practitioners protect themselves for the inevitable problems within cyber environments?

As early as 2003, calls emerged to shift from the traditional views of risk assessment, business continuity planning, and crisis management to an approach where ‘risk management’ is embedded with SCM and other operations—to enable earlier anticipation and mitigation to risks (Jüttner, Peck, & Christopher, 2003). Jüttner also advocated for looking at the points of origin for

risk, which fell into three categories: organization, network, and environment. The links between organizations in the supply chain, the network source, and environmental risks (e.g., natural events, socio-political events) drew particular attention as neglected areas of research (DHS, 2011; Jüttner et al., 2003; G. E. Smith et al., 2007). DHS and several of the national laboratories are making progress with constructing simulations that address portions of the supply chains, in particular the electricity and gas markets, by considering them as complex adaptive systems ([CAS](#)) (Peerenboom & Fisher, 2007). Though these and other [CAS](#) simulations have worked at integrating market reactions into these efforts, there remains a key challenge of integrating nonindustry specific actors as well as human agents into the simulations.

There remains the ongoing challenge of assessing the impacts of contested cyber environments generally (DHS, 2011), and within supply chains specifically. Published consequences from the supply chain community of practitioners are primarily anecdotal in nature (G. E. Smith et al., 2007), or estimations of costs that leave much of their methodology to the imagination of the readers. In short, SCM practitioners are still working on identifying how to assure themselves of the efficacy of their business practices and models in contested cyber environments.

In response to these difficulties and the growing awareness of dependencies on entire networks of related organizations and technologies, supply chain management literature has seen a growth in the idea of disruption management (Pereira, 2009) as championed by Christensen (Christensen, 2006).

Computer Security and Resilience

In many surface-level discussions of computer security, the participants implicitly assume that secure cyber systems are resilient, as no attacks can affect them. A single question will generally disabuse the conversationalists of their simplistic, and naïve notion, “Security from what, for whom, for how long, and at what opportunity costs?” Such a question often results in muttering and stumbling attempts to elucidate an answer. Alternatively, security requirements could drive the discussion (Bishop, 2003) of what constitutes ‘security’. We’ll defer whether to measure, what to measure and how to measure efforts to meet these requirements to later in this dissertation.

Inherent in any security plan should be some residual acknowledgement of possible failure—of one of the dreaded D’s (i.e., destruction, denial, degradation, disruption, and deception). Short of destruction, an organization should be confident in the ability to continue functioning despite the event, ideally during but minimally after the event is over. This is the “recover from” “misfortune or change” portion of the definition of *resilience* at the beginning of this paper. But is the ability to restore functionality what a computer scientist, system developer or programmer perceives when she hears ‘computer security?’ Depending on her background and the context, she could perceive a definition akin to a “reasonable assurance that the complete system will function (only) as required and intended, despite hostile activity” (Horning, 2009). This definition, especially in computer science circles, supports component level design and analysis (Bishop et al., 2011). It’s a reasonable starting place for a profession inculcated with problem decomposition and step-wise refinement. But the definition shortchanges unplanned interactions between technology components as well as unplanned use by humans (Rinaldi, Peerenboom, & Kelly, 2001). Nor does Horning’s definition support a holistic approach to security as a sociotechnical problem, where humans and human organizations interact with components of technology and webs of interconnected technology. This web of interconnected humans and technology is extremely close to characteristics of HROs—minus the tendency of HROs to focus on process before product.

Earlier, I used a definition from Merriam-Webster for *resilience*. The definition implicitly requires that the event or events affecting the system not totally destroy it—pieces and parts maybe, but if the overall system of interest no longer exists, is clearly not resilient, nor was it survivable. Unlike (Bishop et al., 2011; Pimm, 1984), it is important to note that the “or adapts to” portion of definition offers the possibility that the system or systems of interest do not return to pre-event performance! In cases where a system is capable of adapting, it is feasible, and possibility desirable, that the adaptation is permanent, or at least not abandoned at the first opportunity. In addition to Merriam-Webster, a quick review of other definitions, and more importantly ways of assessing those definitions, is appropriate.

Assessing resilience

Assessing resilience is essential for communicating to organizational leaders how its definition applies to their organization. A quick review of ways various industries and research

realms define the concept is fruitful at this point. In ecology circles, generally applied to ecosystems and the study of species, there appear to be two main variants to the definition of resilience (Perrings, 1998). One is a measure of how fast a stable system returns to its equilibrium following a perturbation, and there is no definition of resilience for unstable systems (Pimm, 1984). This makes the concept easily susceptible to measurement, in some unit of time, and requires some idea of whether the measured time is acceptable or not. The other variant assesses the magnitude of perturbation that a system can absorb while still persisting, what Holling referred to as “ecological resilience” (1973). This form of assessment may be measurable, depending on the nature of the perturbation. M&S readily supports Pimm’s definition while Holling’s definition is more applicable to an assessment of cybersystem survivability more than resilience—a lack of persistence implies system destruction, and a destroyed system is clearly not able to recover from or adapt to the perturbation.

Within the computer technology industry and academia, resilience also has multiple interpretations. In the virtualization of computer resources industry, resilience is another flavor of availability (Gilpin, 2008). In this incarnation, the ‘up-time’ of the capability or systems of interest is also easily measured, both during and after cyber attacks or events. This is clearly not a sufficient indicator of adaptability to misfortune or change, as there are plenty of events that could disrupt organizations without making the systems they use nonavailable. Others theorists assert, “Being resilient to an attack, [means] we are stressing the ability of the system to recover from the impacts of this attack or at least to maintain the potential of autonomous recovery” (Bishop et al., 2011). The first half of this definition is akin to Pimm’s return to equilibrium, though Bishop’s has a clear expectation that the equilibrium is equal to the pre-event levels. Such an expectation may be too restrictive, as complex adaptive systems should be able to learn new behaviors, and once learned, they cannot reasonably be un-learned. Nor is it clear that a universal requirement for autonomous recovery is necessary for all organizations.

Some in business management community, view resilience as a capacity for continuous reconstruction and requires systematic preference of innovation over perpetuation of the status quo (Hamel & Välikangas, 2003). This can also be reflected in [Equation 13](#). This definition might be measurable and assessed assuming reasonable estimations of each term are feasible, while organizations desire to decrease the magnitude of the denominator while increasing the

magnitude of the numerator. In other words, reducing the time, expense, and emotional energy associated with transformations is a clear way of increasing resilience in uncertain environments.

$$Resilience = \frac{f(|strategic\ transformation| \times strategic\ transformation_{frequency})}{f(time, expense, energy_{emotional})} \quad (13)$$

Equation 13: Resilience as a function of the magnitude of transformation, the frequency of transformation, time, expense, and emotional energy

The American National Standards Institute ([ANSI](#)) defines resilience as “the adaptive capacity of an organization in a complex and changing environment” with two explanatory notes, one for organizations and one for systems. Note 1 states: “resilience is the ability of an organization to resist being affected by an event or the ability to return to an acceptable level of performance in an acceptable period of time after being affected by an event.” Note 2 states “resilience is the capability of a system to maintain its functions and structure in the face of internal and external change and to degrade gracefully when it must” (American National Standards Institute (ANSI), 2009). All three of these slightly different flavors do not immediately lend themselves to straightforward measurement or assessment. Organizations have to have a coherent model of their functions and structure to support this definition or find and use measurable proxies for these concepts.

The US government is also not immune to creating definitions, as the Department of Homeland Security ([DHS](#)) defines resilience as “for cyber defense purposes, having sufficient capacity to simultaneously collect or receive and assess security information, execute any [ACOA](#) (Automated Courses of Action] make alterations to the ACOA as needed, and sustain agreed upon service levels” (DHS, 2011). This definition, like the ANSI definition, presupposes a way of measuring organizational capacities as well as predicting the impacts of various events on those capacities. While definitions must of necessity be concise, the DHS definition simply begs for clarification and expansion—which requires another 29 pages to explicate.

What is clear from discussion so far is that resilience to contested cyber environments means a number of things to different audiences—there is no singular definition applicable across all possible contexts. What is apparent however, is interested audiences should not treat resilience as an isolated static measure independent of time. Instead, it incorporates time, effects of perturbations, and the maintenance of function during perturbations and adaptation to those perturbations. There are no Newtonian laws of adaption that require the adaptations be

permanent. Nor are there universal asymptotic equations constraining adaptations to pre-perturbation levels of performance. These realizations lead us to a short review of non-HRO treatments of organizations learning and behavior—how collections of people learn and behave, especially in stressful environments.

Organizational Learning and Behavior

Industry and academia have well established that organizations learn and Huber's literature review does an excellent job reviewing the history of experiential learning of organizations (Huber, 1991). There is significant evidence that the learning is nonlinear, is often based on myths and stories, and is at times mal-adaptive (Cyert & March, 1963; B. Levitt & March, 1988; March, 1991). There is also evidence that organizations behave differently in ambiguous and unambiguous environments (March & Olsen, 1975; Padgett, 1980) as well as evidence that individuals call on different relationships and information gathering mechanisms in times of uncertainty and ambiguity (Saint-Charles & Mongeau, 2009). The entire field of organizational learning and behavior is well beyond the scope of this review, so I constrain the remainder of this section to research on organizational learning and behavior that includes organizations' information technology and cyber resources.

Researchers have shown organizational structure (both formal and informal structure) effects learning and adaptation. Padgett found that the heads of hierarchies can best influence their organizations by focusing more on who they pick to run their various subordinate organizations than on trying to make decisions themselves (Padgett, 1980). Organizational structure, the relationships and links between the members of the organization and links between organizations, also plays a role in learning. Hierarchies, though non-optimal in many measures of organizational performance, tend to be more resilient to certain types of turbulence (e.g., personnel turnover/turbulence) than other structures (Kathleen M. Carley, 1992). The reader may also recall the seeming paradoxes associated with HRO research contrasted with traditional organization theory. The first is HROs tend to use significant quantities of advanced technology that requiring specialization yet HROs also exhibit high degrees of interdependence that requires generalist understanding. The second is that HROs tend to have high task interdependency despite operating in high variability environments (Roberts, 1989, 1990).

Wade & Hulland, in their review of organizational learning and information technology literature (2004), used the resource-based view ([RBV](#)) of organizations. In this view, IT systems are tangible assets while the knowledge to run those systems, the knowledge stored in those systems about how the organization runs and operates are capabilities of the organization. He also discusses multiple research products that demonstrate that IT systems, and the capabilities represented in them often play distinct roles in gaining initial competitive advantage and sustaining long term advantage (Wade & Hulland, 2004). Unfortunately, Wade, Huber, nor Damanpour's (1991) literature reviews include research on IT dependent or enabled organizations when those resources are degraded or no longer available. Neither does the meta-analysis model built by Damanpour's (Damanpour, 1991) integrated inclusion then disruption of cyber resources.

Research on the use of information technology, or other cyber capabilities, to enable communications within organizations, especially to facilitate adaptation also has a robust history. Empirical studies on adoption of information technology go back over thirty years (Orlikowski & Gash, 1994). The data sample driving this review has over 130 articles with more than 100 citations each in the data sample dealing with technology relating to adaptation and learning. Miller showed that even in primitive environments, any communications mechanism will improve performance and having more robust communications will increase performance (J. H. Miller & Moser, 2004), while Carley (1995) and Haythornthwaite (2005) have studied and demonstrated that mass communication technologies can encourage common homogeneous culture, but only as an eventuality—that the near term can suffer in increase in heterogeneity and loss of consensus. Martin et al asserted via simulation that the degree of information error and the degree of communications network intermittency interact to reduce decision accuracy in organizations across random structural designs (Martin, Morgan, Joseph, & Carley, 2010). Interestingly, they discern statistically significant impacts on decision accuracy by communications media only in the extreme cases of information error (e.g., all accurate, all inaccurate) (Martin et al., 2010), which implies that organizations are resilient along this measure of performance. This finding of accurate learning and performance being independent of organizational structure is in contrast to Carley's determination that training and structure are statistically important, as is the location of the communication's breakdown (Kathleen M. Carley, 1991).

Surprisingly, there appears to be very small quantities of research directed at use of IT in degraded or destroyed environments. Among the studies of adaptation to disruption and loss of communications networks are those focused on flow disruption (Saltysiak & Levis, 2012) and development of decision support systems (Saltysiak & Levis, 2012; Snediker, Murray, & Matisziw, 2008) and efforts to setup taxonomies of mission impacts from cyber events (Grimaila, Mills, & Fortson, 2013; Musman, Temin, Tanner, Fox, & Pridemore, 2010).

A close cousin to organizational learning is organizational assessment. There is a field of science that has grown up around assessing organizations, what they have learned and their effectiveness at their missions. Unfortunately, organizational effectiveness, in addition to going through a near death experience in the early 1980s, has the problem of exactly who is measuring what and to what standards (Cameron, 1986). In addition, like resilience, there is the debate about when to study—before events or after. In the case of organizational effectiveness, researchers tend to examine well-established companies with less emphasis on new and dynamically expanding organizations (Quinn & Cameron, 1983). In the case of examining resilience to contested cyber environments, researchers focus on the direct monies loss, estimates of future monies missed, and estimates of indirect costs such as damage to reputation or trust. These have the disadvantage of being poor and opaque proxies for organizational impacts (DHS, 2011; Jüttner et al., 2003). Judging by scarcity of published materials, researchers are not yet looking at the ways the companies adapted to the contested environment and demonstrated resilience to their misfortune(s).

As noted by Huber (1991), the organizational learning literature has an enormous breadth, and over 20 years later there are still gaps to explore. The documents in the collected sample, plus additional and refined searching, have still lead to a paucity of research of organizational learning and adaptation to contested cyber environments. This paucity seems to be a natural area of research to bridge between resilience engineering, risk management, and cyber risk management.

Social Network Analysis, Metanetworks, and Dynamic Network Analysis

The representation of collections of humans interacting with other humans, and the systematic study of those representations is an old and widely practiced field. Since the mid-twentieth century, a common description of this study has earned the name Social Network

Analysis (Freeman, 1977, 1979). These representations most frequently take the form of single mode networks, or graphs comprised of links and nodes. In single mode networks, each node is a person and the people under study belong to a single class—there are not distinct types of people (Wasserman & Faust, 1994). Two mode networks within traditional SNA usually refers to the interactions of two distinct types or groups of people (Wasserman & Iacobucci, 1991), such as doctors interacting with nurses, or intravenous drug users interacting with their sexual partners (Williams & Johnson, 1993). A sample of SNA metrics that researchers apply to the graph models of human interactions is below in [Table 8](#) drawn from (Kathleen M. Carley, 2011). Multimode analysis usually supports a richer understanding of the human groups of interest than single mode and I provide a brief review below.

Metanetworks and Metanetwork Analysis are an extension of SNA and a modification of the definition of multimode network. In metanetworks, multimode networks are networks with numerous distinct node types, e.g., agents, resources, tasks, and knowledge. From the three-node type instantiation (Krackhardt & Carley, 1998) it progressed to a four-node version (Kathleen M. Carley, 2002a; Kathleen M. Carley & Krackhardt, 1999) similar to that shown below in [Figure 34](#) to the nine (9) node-type version shown in [Table 7](#) (Lanham, Morgan, & Carley, 2011a) derived from (Kathleen M. Carley, 2002a; Diesner & Carley, 2005) which is its current state.

Table 7: Nine (9) node metanetwork and their internode link interpretations¹⁰

Networks		Node Types							
Node Types	Agent	Knowledge	Resource	Task	Event	Organization	Location	Role	Belief
	Agent “Who knows who”	Knowledge “Who knows what”	Capabilities “Who has what”	Assignment “Who does what”	Attendance “Who attends what”	Membership “Who belongs to what org”	Agent Location “Who is where”	Role “Who has what roles”	Belief “Who believes what”
	Knowledge	Information “What informs what”	Training “What resources are needed for training”	Knowledge Requirements “What knowledge is task critical”	Education “What event teaches what”	Organizational Knowledge “What org knows what”	Knowledge Location “Where is what learned”	Role Requirements “What must be known to perform what”	Knowledge Influence “What knowledge informs what?”
	Resource		Substitution “What can replace what”	Resource Requirements “What tasks require what”	Event Requirements “What events require what”	Organizational Capability “What org can do what”	Resource Location “Where is what”	Role Requirements “Who needs what resource to do what”	Resource Beliefs “What beliefs are required to use what”
	Task			Task Precedence “What must happen before what”	Event Agenda “What tasks occur at what?”	Organizational Assignment “What org does what”	Task Location “Where is what done”	Role Assignment “What roles do what”	Belief Requirements “What beliefs require what tasks”
	Event				Event Precedence “What events happen before what”	Organizational Responsibility “What org is putting on what”	Event Location “Where is what event”	Role-Event Requirements “What roles are often present at what”	Belief Attendance “What beliefs influence participation at what”
	Organization					Inter-Organization “What org works with what”	Organization Location “Where is the organization”	Organization Role “What org has what roles”	Organizational Culture “What beliefs are common”
	Location						Proximity “What is near what”	Location Roles “What roles are common where”	Significant Locations “Where is associated with what beliefs”
	Roles							Inter-Role “Who knows what”	Significant Roles “What roles are associated with what beliefs”
	Beliefs								Belief Influence “What beliefs influence what”

¹⁰ (Lanham, Morgan, et al., 2011a) and derived from (Kathleen M. Carley, 2002a; Diesner & Carley, 2005)

Table 8: Common SNA metrics and their interpretations

Measure Name	Definition	Meaning	Usage
Degree Centrality	Node with most connections	In the know	Reducing information flow, ID sources of intelligence
Betweenness	Nodes in most best paths using symmetric data	Connects groups	Typically has political influence, though may be too constrained to act
Eigenvector centrality (Bonacich, 1972a, 1972c)	Nodes connected to other well connected nodes	Strong social capital	ID nodes that can mobilize other nodes
Closeness	Nodes closest to other nodes	Rapid access to all information	ID nodes to best acquire/transmit information
Betweenness Centrality (Freeman, 1979; Freeman, Roeder, & Mullholland, 1979)	High betweenness, low centrality	Connects otherwise disconnected groups	Go-between; Reduction in activity by disconnecting groups
Authority Centrality (Kleinberg, 1999)	Sum of hub scores from in-link / hub score	Subject Matter Expert	ID nodes that others recognize as SME on one or more subjects

In [Figure 34](#), a four node metanetwork is shown. Each oval represents one of four node types, with decision making units ([DMU](#)) being equivalent to “decision making unit.” Implicitly in this diagram, there exists links amongst DMU nodes, intra-task links, intra-resource links and intra-knowledge links. Those intra-task links represent, usually, task dependencies or task precedence networks. Intra-resource and intra-knowledge links can also represent resource and knowledge dependencies or even compositions or aggregations of resources and knowledge. The various labeled relationships are depicted unidirectional, but there is no definitional requirement that a modeler must maintain such a convention. The development and refinement of metanetwork model construction and analytical development has been a hallmark of Carley’s research group at CMU’s CASOS (Kathleen M. Carley, 2003).

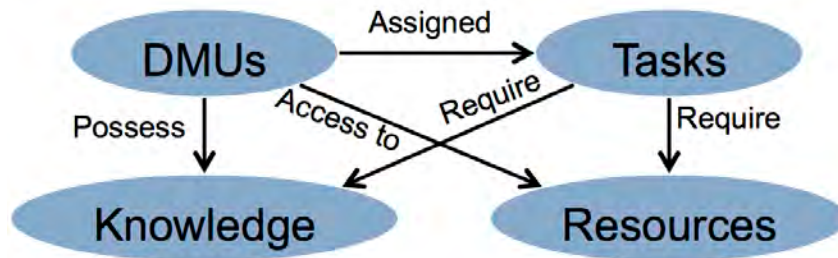


Figure 34: Four-node metanetwork

Metanetwork notation in Carley et al.'s research, as well as this dissertation is below.

$\mathbb{A} = \{Agent_1 \cdots Agent_m \mid m \geq 1\}$, the nonempty set of all agents in the metanetwork

$\mathbb{K} = \{Knowledge_1 \cdots Knowledge_j \mid j \geq 1\}$, the nonempty set of all knowledge in the metanetwork

$\mathbb{R} = \{Resource_1 \cdots Resource_k \mid k \geq 1\}$, the nonempty set of all resources in the metanetwork

$\mathbb{T} = \{Task_1 \cdots Task_k \mid k \geq 1\}$, the nonempty set of all tasks in the metanetwork.

$\mathbb{AA}(i, j) = \begin{cases} > 0 \text{ or } 1 & Agent_i \text{ linked to } Agent_j \\ 0 & \text{Otherwise} \end{cases}$, matrix of relationships between agents

$\mathbb{AT}(i, j) = \begin{cases} > 0 \text{ or } 1 & Agent_i \text{ linked to } Task_j \\ 0 & \text{Otherwise} \end{cases}$, matrix of agents with their assigned tasks

$\mathbb{AR}(i, j) = \begin{cases} > 0 \text{ or } 1 & Agent_i \text{ linked to } Resource_j \\ 0 & \text{Otherwise} \end{cases}$, matrix of agents with access to resources

$\mathbb{AK}(i, j) = \begin{cases} > 0 \text{ or } 1 & Agent_i \text{ linked to } Knowledge_j \\ 0 & \text{Otherwise} \end{cases}$, the matrix of knowledge possessed by agents

$\mathbb{TK}(i, j) = \begin{cases} > 0 \text{ or } 1 & Task_i \text{ linked to } Knowledge_j \\ 0 & \text{Otherwise} \end{cases}$, the matrix of tasks linked to their supporting knowledge

Carley et al have also been vigorously applying the metanetwork perspective to over time models (Kathleen M. Carley, 2003; Kathleen M. Carley & Lee, 1998; Lin & Carley, 1997; Schreiber & Carley, 2005) at the same time that longitudinal network analysis remains a vigorous field of research for both understanding network evolution (Graham, 2005; Skvoretz & Fararo, 1995; Ter Wal & Boschma, 2007; Tushman & Romanelli, 1985; Zeggelink, Stokman, & Van de Bunt, 1996) as well as network change detection (McCulloh, 2009; I. McCulloh & K. M. Carley, 2008; I. McCulloh, Daimler, Eric, & K. M. Carley, 2008). When adding the time dimension to metanetworks, the definition of dynamic network analysis becomes clear: the study of multimode and multiplex networks over time. The expansion of quantifiable measures into the metanetwork framework supports the calculation of generalized measures across the multimode network such as performance as accuracy, shared situation awareness (Graham, 2005; Graham, Schneider, Bauer, & Bessiere, 2004), knowledge and communication congruence and workload and cognitive demand (Kathleen M. Carley & Pfeffer, 2012a, 2012c). Dynamic metanetworks,

like their SNA antecedents, also support bi-directional links though the various SNA software products treat this data differently and the researcher must decide if the calculation of the metric against the available data is meaningful (Wei, Pfeffer, Reminga, & Carley, 2011).

Modeling and Simulation

As discussed in the “[Supply Chain Management and Resilience](#)” section, incorporating uncertainty into supply chain models and attempts to understand HROs are fairly robust fields of research (Pereira, 2009). Where SCM modeling still needs to grow is the explicit inclusion of contested cyber environments as a cause of uncertainty. Within DHS sponsored research, simulation of disruption of critical infrastructures with SymSuite (Brown, Riolo, Robinson, North, & Rand, 2005), SMART++ (North, 2000), and RINSE (Leblanc et al., 2011) is well advanced for exploring inter-dependencies of complex physical infrastructures. Incorporating socio-political components into any of the tools does not appear to be a part of their follow-on work.

Modeling complex adaptive systems ([CAS](#)) is also a healthy area of research applied to a great many fields, from finance markets (Markose, 2005) (see (Hommes, 2001) for a markets as CAS literature review) to critical infrastructure (Rinaldi et al., 2001). These efforts have ranged from exploring organizational designs to cope with communication breakdowns (Kathleen M. Carley, 1991; DHS, 2011) to sociotechnical models such as OrgAhead (Effken, Brewer, Patil, Verran, & Carley, 2005; Lee & Carley, 2004; Louie, Carley, Haghshenass, Kunz, & Levitt, 2003), SimVision (Emery, 2002; ePM, 2012; R. E. Levitt & Kunz), and Construct (Kathleen M. Carley, Joseph, Lanham, Morgan, & Kowalchuck, 2014; B. Hirshman, St. Charles, & Carley, 2011; B. R. Hirshman, Kowalchuck, & Carley, 2008)

OMNeT++ (OMNeT++ Community, 2012) and NetSim (ns-2) are examples of technology-focused, discrete event simulation environments that enables M&S of networks at the technical system and component level: networked devices, communications channels and messages on those networks (2012). There are numerous other examples of technology-focused simulations, from OPNET Modeler from Cisco, to University of Illinois at Urbana-Champaign’s Real-Time Immersive Network Simulation Environment ([RINSE](#)) (Leblanc et al., 2011), to the seventeen network emulators listed in (Lochin, Pérennou, & Dairaine, 2012), that all provide evidence of the field maturing greatly since Cohen’s lamentations about the sad state of cyber

security M&S (F. Cohen, 1999). With these capabilities, researchers are able to construct models of technical components of infrastructure, as well as organizations' sets of other cyber resources and assets (e.g., servers, terminals, other IP-enabled devices). With those models they can choose various forms of network degradation (e.g., congestion from a denial of service attack, loss of packets from a noisy transmission medium or other adversarial effect), analyze the effects on the effected systems, the network as a whole, as well as identify 2nd and 3rd order effects in their models.

Process-level modeling of business processes has also been, and remains, an active field of research. Colored petri-nets (Levis, Carley, & Karsai, 2011) and colored petri-nets over time (Pflanz, 2012; Pflanz & Levis, 2012) as well as time-influence nets (Levis et al., 2011) have incorporated various levels of cyber attacks into their efforts to gauge impacts on organizational capacities and decision time lines. Machine-level processes, independent of human-controlled actions, have also been explored in the development of rate control services (Gligor, 2005) and load-balancing redirection (Pai et al., 1998; Wang, Pai, & Peterson, 2002). Human-enabled process modification (e.g., employing off-line backup capacity) is also apparent in (Pflanz, 2012; Pflanz & Levis, 2012) as a way of assessing the sustainability of time-sensitive missions in cyber degraded environments. What these process-based models omit though are the individual agent level adaptations to the environment—disaggregating agents is not a feature of the above modeled processes and flows.

Each of these tools, to greater and lesser degrees, can help construct scenarios where researchers or analysts can model an organization's technology assets and assess its technical resilience to the chosen perturbations. But what of the nontechnology assets? Every organization has people, processes, resources, data, information and tasks that, to some degree or another, must go on even during "misfortune or change." RINSE has been used by the USG during a *Livewire* exercise (Leblanc et al., 2011), the DoD's Bulwark Defender attempts to train staffs and commanders in process adjustment and efforts to inject communications effects servers into exercises continue (Wihl, Varshney, & Kong, 2010)—though the risk of participants' misperceiving an attack as a simulation malfunction is ever present. There is an apocryphal story in DoD simulations community Incorporating that very real risk.

Exercise participants in a virtual and constructive simulation, on perceiving a malfunction in the simulation, headed to lunch. On their return from lunch, they

discovered the enemy had destroyed their simulated units and equipment. On demanding an explanation from the simulation support staff, the players learned they had misdiagnosed the cause of several events, failed to report or explore the possible causes of the events, and subsequently had their units die as a result of leaving their workstations.

Multimodel modeling is another technique to assess organizational resilience in contested cyber environments. Researchers use multiple models to address multiple portions of the problem space: technical details, information diffusion, social influence, forecasting effects, and forecasting the efficacy of remediation's and adaptations. These models exchange information about their own inputs and outputs to help enrich the overall modeling effort (Kathleen M. Carley, Geoffrey P. Morgan, Michael J. Lanham, & Jrgen Pfeffer, 2012; Kathleen M. Carley, Geoffrey P. Morgan, Michael J. Lanham, & Jürgen Pfeffer, 2012; Elder & Levis, 2010). These works have shown a way to having models work in tandem, though they are not inter-operable per se. The models share information, and most importantly can serve as means of validating the outputs of each other—when systems with very different internal processing generate congruent results, analysts can have higher confidence in the feasibility of the results. Examples of the tools used in the above modeling efforts include: OMNet++, Construct (an agent based belief and information diffusion simulation) (Frantz & Carley, 2007; B. Hirshman et al., 2011), CAESAR III (a C2 design tool) (Levis & Perdu, 1996), and Pythia (a timed influence net simulation) (Wagenhals & H., 2001; Wagenhals, Levis, & McCrabb, 2003; Wagenhals & Wentz, 2003). With the combination of these tools, researchers were able to assess multiple aspects of resilience: the ability to continue functioning during a perturbation, assess the magnitude of various effects within the modeled organizations, and forecast the adaptations needed by the organization to perform as best it could in its simulated environment.

Yet another example of multimodeling was the co-use of ORA™ and MONOPATH. In this merger of tools that analyze social networks and telecommunications networks, researchers found that including message passing paths from social-networks in a resilience analysis, organizations can improve the message delivery by a factor of five without gross changes in end-to-end latency (Bigrigg, Carley, Manousakis, & McAuley, 2009).

An example of a process centric M&S approach to assessing resilience is Pflanz's work with colored petri nets (Pflanz, 2012; Pflanz & Levis, 2012). With this approach, a modeler builds information flow paths and then executes them to assess the model against various

measures of performance and effectiveness. With timing information included in the information path, this technique has shown that time-sensitive missions (e.g., a military unit's 'time-sensitive targeting' using GPS-enabled munitions) are not supportable when key portions of the model are 'denied' (e.g., GPS jamming). He also showed that organizations that are IT enabled may have no reduction in capacity with one attack on their systems, though they have zero residual capacity to absorb any additional misfortunes.

M&S of contested cyber environments tends to fall into three camps. The first is the discrete event simulation that operates at bit/byte-level and/or the telecommunications-network-level. These simulations help computer scientists and engineers identify specific failures of components, protocols, or individual systems and IT engineers and organizations identify actual or potential portions of the network that exhibit undesired behavior. They can help simulate the technical failures associated with a contested cyber environment, but do not incorporate any of the cognitive learning and adaptation functions of the organization. The second camp is the organization model that supports examination of the organization(s) at varying degrees of aggregation from the individual person up to teams and groups—but those rarely incorporate explicit and implicit dependencies on IT and information residing on that IT. Even more rarely do those organizational simulations support the experimental analysis of how the individuals, teams, and organizations as a whole adapt to the degradation or destruction of the IT assets they perceive they are dependent on. The third camp is a process-centric set of modeling capabilities. In this camp, detailed, time-dependent models are built per process-of-interest. When the models are complete, what-if scenarios offer insights to possible effects of future scenarios.

Each of the above camps adds value to the M&S communities to which they belong. Unfortunately the absence of an ability to model the cognitive adaptations of organizations to the use and loss of their cyber capabilities remains a capability gap in the research of organizational resilience!

Conclusions

In the abstract and Introduction chapter, I discuss four demands leaders should place on their organization to increase their assurance of resilience to contested cyber environments. This chapter has addressed the first of those four demands: leaders should require analytical and empirical assessments that incorporate organizational and individual cognitive complexities. The

chapter enumerates not only the reasons for the assertion, but identifies gaps in existing research into organizational resilience in contested cyber environments.

I have developed an argument to justify the importance of studying organizational resilience in contested cyber environments. There should be few reasons for arguments against the notion that modern, 21st century organizations, especially in the industrialized first world, are increasingly using their information technology and cyber capabilities in ways they had not predicted. As a corollary generalization, those organizations are challenged in fully appreciating the multitudes of 2nd and 3rd order consequences of such use.

Despite this growing use of IT, I also developed a case that doomsday, apocalyptic, and other predictions of existential threats are intemperate, and place the advocates for those views in a less credible position than they could otherwise maintain. Instead, I set the stage for a reasoned and deliberate inter-disciplinary study of organizational resilience in contested cyber environments—both man-made and naturally occurring.

I then transitioned to an explanation of how I collected sample articles and texts associated with what I had initially assessed would be primary candidates for inter-disciplinary studies: supply chain management, business continuity, general risk management, cyber risk management, organizational learning, organizational behavior, and modeling and simulation. Through semantic network analysis and network analytics, I demonstrated that 13,000 collected articles show weak connections between cyber risk management and risk management, weak connections between general/global risk management and organizational learning, and an even weaker link between organizational resilience and organizational innovation.

Next I offered a literature review of cyber risk management, organizational resilience, organizational learning, as well as modeling and simulation applied to each of those three areas. The literature reviews, while necessarily brief, illustrated that despite the breadth of research in each area there are far fewer areas of commonality and shared references than intuition originally suggested. There are gaps between the fields of research of organizational learning supported by IT and the loss of that IT once the organization has grown accustomed to it. There are gaps in the M&S support to both technical dependency modeling and cognitive modeling of humans using the technology. Finally there are gaps between the risk management communities (cyber and

general) and organizational learning—as evidenced by the continued successes bad actors enjoy exploiting human vulnerabilities in organizations.

Reliance on a set of capabilities represents a risk to organizations that have few or no alternatives. Mitigating risk is a natural outgrowth to being aware of it, and preparing for the eventuality of undesired events should also be a natural part of organizational operations. With practice, an organization gains confidence in its abilities—it builds an experiential store of knowledge from which it can draw actual lessons as well as extrapolate to unfamiliar situations. Practice is, of course, expensive, opening the door to the use of M&S as an expense mitigation compared to live experimentation with organizational elements and assets otherwise occupied with daily missions. With confidence and ability, organizations can assure themselves, their leaders, and the organizations they interact with that they are resilient to misfortune, that they can adapt and overcome adversity.

Data and Models

Introduction

This chapter will introduce the methodology for collecting data for use in this dissertation. It will also introduce the process and contributions for rapidly turning that data into multimode (multiple node types) and multiplex (multiple types of links between nodes) organization models for assessing mission assurance in contested cyber environments. The chapter will also present processes and rationales for the modifications to the collected data to transform the empirical models into inputs for the agent based simulation, Construct (Kathleen M. Carley et al., 2014). In the literature review and research for this dissertation, I have not found evidence of using this methodology and its generalization for organizational modeling in cyber contexts. Nor have I uncovered evidence of its application to DoD doctrinal source material and the use of its outputs in mission assurance contexts. This rapid modeling approach represents one of the principal contributions the dissertation to the field of mission assurance and organizational resilience to contested cyber environments.

Prior to providing the detailed discussion of the data collection and processing, it is useful to see a high level view of what will happen to that data in the workflow of the dissertation; I will use this diagram through the dissertation to relate each chapter to its relevant piece of the workflow. [Figure 35](#) provides such a view, with the left most rectangle representing this chapter, and the blue ovals representing supporting or specific activities. The Data-to-Model ([D2M](#)) process (Kathleen M. Carley, Bigrigg, et al., 2011; Lanham, Morgan, & Carley, 2014; Lanham, Morgan, Carley, & Levis, 2011) is a defined sequence of steps for researchers to use, with the support of automation, to rapidly ingest unstructured and semi-structured data and convert that data into SNA and metanetwork-based models for analysis using graphic theoretic techniques. The process is in the rectangle labeled *D2M/Define Organization* in [Figure 35](#). The [Network Analytics and Resilience](#) chapter provides the detailed discussion of metrics against the static models generated within the D2M—the *Calculate Metrics* rectangle in [Figure 35](#). The chapter for [Agent Based Models and Modeling](#) addresses the justifications for using Agent Based Models and the augmentation needed to take the output of the D2M block and provide input to the Construct Simulator block. The in-depth discussion of Performance as Accuracy ([PaA](#)) and Shared Situational Awareness ([SSA](#)) is also in the [Network Analytics and Resilience](#)

chapter. A repeat of the block labeled *Calculate metrics* occurs for the outputs of the simulation in the [Simulations](#) chapter. The block labeled Compare gets its due in the [Simulations](#) chapter as well as the [Heuristics](#) chapter.

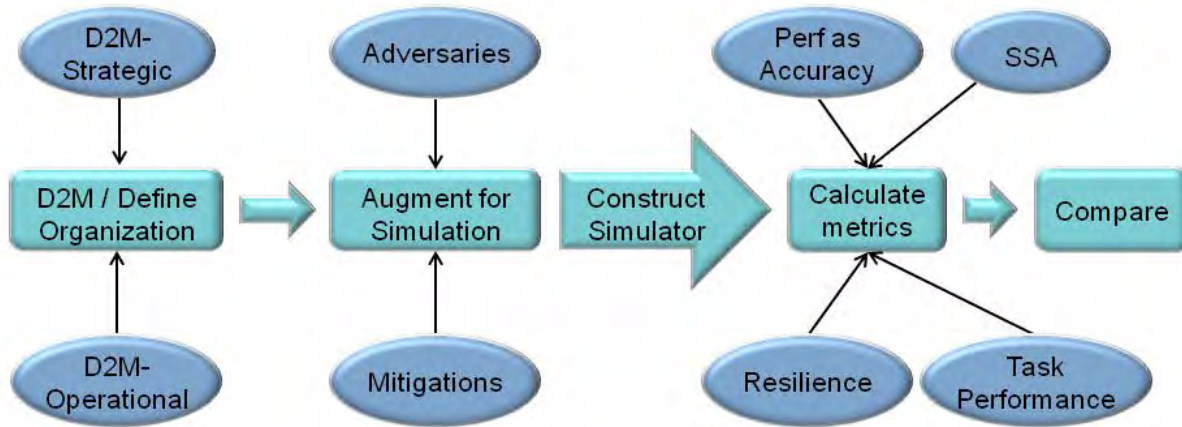


Figure 35: Stylized dissertation workflow

Organization—a working definition

For the purposes of this dissertation an organization is a collection of decision-making units ([DMU](#)) (aka specific agents) and roles (aka general agents). The organization also includes the DMUs’ supporting IT systems and capabilities as well as other resources. The organizational definition also includes the tasks and knowledge of the organization’s members as well as their beliefs, specified events and enumerated actions. Each of the above named categories of entities is, in their respective models, a node type. Any arbitrary node is a specific instance of a node type. The model, to be accessible to graph theoretic techniques, also includes the relationships between these various nodes and their node types. There may also be multiple relationships in that two different edges representing two distinct types of relationships may link nodes together. Subsequent paragraphs will explain how I gathered data to construct the multimode and multiplex models of organizations under test.

There are two types of organizations in the dissertation, both derived from the D2M process: strategic and operational. The two are shown in [Figure 35](#) as the two leftmost ovals, with the rest of the workflow standardized and applied to both models. I present the data sources for the D2M derived models next.

Organizations' Self-Documentation

Organizations frequently describe themselves in various ways, not all of which are aligned with the perceptions of their members or nonorganizational observers. A common mechanism for an organization to describe itself is in terms of its mission statement: for whom does it work, what it does, why it does what it does, when does it do its work (or to whose schedule), where does it do its work, and how does it accomplish its work. Mission statements, if they exist, are excellent starting points for new arrivals to the organization as well as observers to gain a level of understanding about the organization.

Another mechanism organizations use to describe themselves are documents they write for their various intended audiences. A vision statement from the chief executive officer ([CEO](#)), or other principal leader, targets not only outsiders with whom the company interacts or wants to interact, it can serve as a common point of reference for internal audiences. A combination of mission statements and vision statements frequently serves as the beginning of organizational culture—a shared set of knowledge (Kathleen M. Carley, 1994). They can also serve as the starting point for organizational modeling as well as help scope the models in this dissertation.

An additional way organizations describe themselves is via organization charts. These often represent subsets of people and suborganizations as blocks connected via lines. The lines and the relative position of the blocks often indicate direct and indirect reporting chains (e.g., chains of command), information flows, and functional specialties. These charts assist organizations' formal depictions of themselves and relationships between included elements or people. What the charts rarely depict is the myriad of individual persons in each subelement—the autonomous humans that ideally subscribe to and help implement the organizations culture and mission.

The Data to Model Process—an Overview

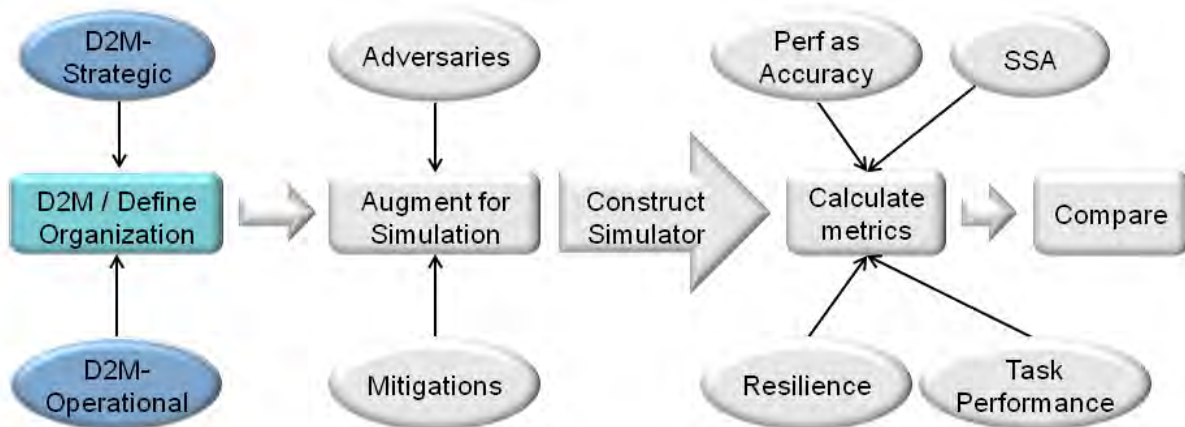


Figure 36: Dissertation workflow data to model (D2M)

Using [Figure 36](#) as a breadcrumb, the [D2M process](#), is the first step in the creation of organizational models to use to answer the questions of interest in this dissertation.

From the mid-1970s onward, there has been a growing effort at developing a theory of semantic networks. The central idea in semantic network theory is that collections of disambiguated words (as nodes) related to each other (using links) can represent human knowledge (W. Woods, 1975) in semantically meaningful ways. Using networks also helps researchers subject the semantic networks to rigorous mathematical graph theoretic approaches.. To a large degree, this effort was in support of the then-expanding field of artificial intelligence ([AI](#)) and bridging the gaps in approaches between linguists and AI researchers (Hartley & Barnden, 1997). By the early 1990s, semantic analysis had matured to the point that meanings were measurable on multiple dimensions (e.g. connectivity, conductivity, and consensus (Kathleen M. Carley & Kaufer, 1993)) as well as supporting research into multiple mechanisms to visually represent such networks (Gloor & Zhao, 2006; Hartley & Barnden, 1997).

By using text documents generated by various organizations and authors as sources for semantic networks, it is feasible for a researcher to gain insight not only into the possible overlaps in content but also perceptions of overlap in responsibility (Ekstrom & Lau, 2008) for organizational tasks. Semantic networks can also help represent the authors' mental models as they wrote the various documents (Diesner & Carley, 2005, 2011) as well as help automate the acquisition of relational information for members of an organization (Gloor & Zhao, 2006; Mergel, Diesner, & Carley, 2010).

As previously mentioned, the [D2M process](#) (Kathleen M. Carley, Bigrigg, et al., 2011; Kathleen M. Carley, Columbus, Bigrigg, Diesner, & Kunkel, 2011; Diesner & Carley, 2004; Lanham et al., 2014) is a rapid machine-assisted transformation of a collection of text documents (labeled *DoD Doctrine and Pubs* in [Figure 37](#)) into a metanetwork model (Panzarasa, Carley, & Krackhardt, 2001). It includes an ontological classification scheme of nine (9) categories into which each concept will fit. Through this process, the researcher constructs an indirect model of the collected documents. These models are reflections of the concepts and ideas the authors of the input documents were attempting to communicate to their respective audiences.

The D2M process, as applied to this problem domain and source material domain, required adaptation of the methods the sources cited above describe. Shown in [Figure 37](#), the process began with a thesaurus that CASOS staff, faculty, and students developed using both hand encoding as well as machine learning techniques (i.e., conditional random field ontological categorization). Through a D2M Wizard within AutoMap, this figure represents the completely automated¹¹, first-round process of text cleaning, removal of stop words, and other processing steps performed for the user. From this wizard, AutoMap generates multiple products a researcher uses to determine if the model of the text is sufficient to their needs. The products include semantic networks, often referred to as collocation networks of words within a sliding window of specified size, suggested ngram lists, suggested review lists, and suggested acronym lists. A key product is the first generation metanetworks (per text if of interest, as well as the union of all texts' models).

It is frequently the case that the first generation metanetwork is insufficiently developed to explore or resolve questions of interest, and that was certainly true in this dissertation. For these cases, the human-aided [D2M process](#) begins with *thesaurus refinement* as shown in [Figure 38](#) and linked to [Figure 37](#) via the “A” off-page connector in the flowchart. To develop a second (2nd) through nth iteration of a metanetwork that can help resolve the research question of interest, I used the defined process labeled “1” in the [Figure 38](#) flowchart. This requires extracting the concepts from the Wizard generated lists into a dissertation thesaurus. For each of the three organization models, discussed in the next section, I developed an additional thesaurus to adjust

¹¹ AutoMap processing time per file for some steps is approximately logarithmic in file length. Because of this growth in processing times, [Figure 37](#) depicts a subprocess whereby I combined the retrieval of the files as pdfs, the extraction of text from those pdfs using pdftotext, and the splitting of the extracted text files into chunks no bigger than 64KB.

the overall scope of the model and its contents. While developing these thesauri, it was necessary to develop two (2) capabilities not yet in AutoMap: the application of regular expressions as well as case sensitive application of thesauri.

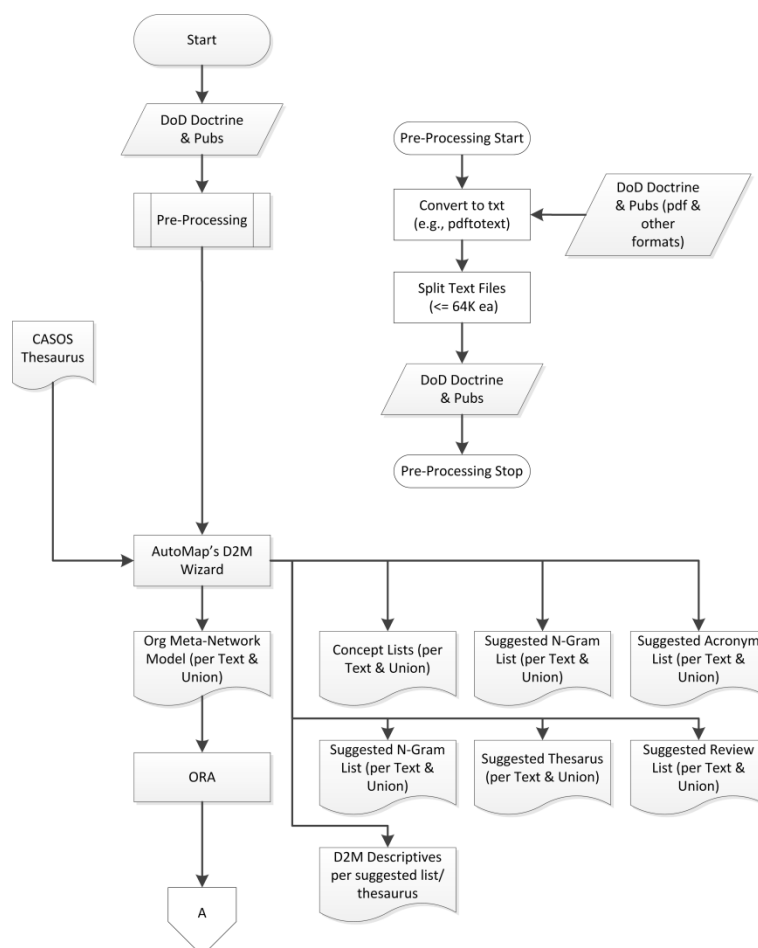


Figure 37: Data to model wizard applied to any input corpus

DoD self-documentation has numerous references to other documents that frequently follow patterns of use. Through development and application of Perl Regular Expressions to convert these document identifiers into ngrams, it was my expectation that I would be able to identify which of the sources appeared to have the most impact on the overall model development. DoD document authors also frequently use acronyms in all capital letters that overload standard English words in lower-case (e.g., [IT](#)/it, [WHO](#)/who, [POP](#)/pop). To cope with these two characteristics of the input corpus, I modified the standard CASOS [D2M process](#) by adding the defined process labeled “2” in the [Figure 38](#) flowchart. The details of these steps are in the [Pre-processing DoD corpus](#) section of [Appendix 1](#).

Of particular note, at the end of this overview are some of the specific tangible deliverables of the dissertation. The specific deliverables, as shown in [Figure 38](#), are the pre-processing scripts for regular expressions and case sensitive application of a thesaurus, the *dissertation thesaurus*, *acronym/case sensitive thesaurus*, and the *model-specific thesaurus*. All of these deliverables are free of restrictive intellectual property rights as a work product of the USG, though I do ask that future users of the deliverables acknowledge the products' origin! I have also made these thesauri and the scripts available on my personal web page at http://www.andrew.cmu.edu/user/mlanham/nonpeer.shtml#dissertation_support.

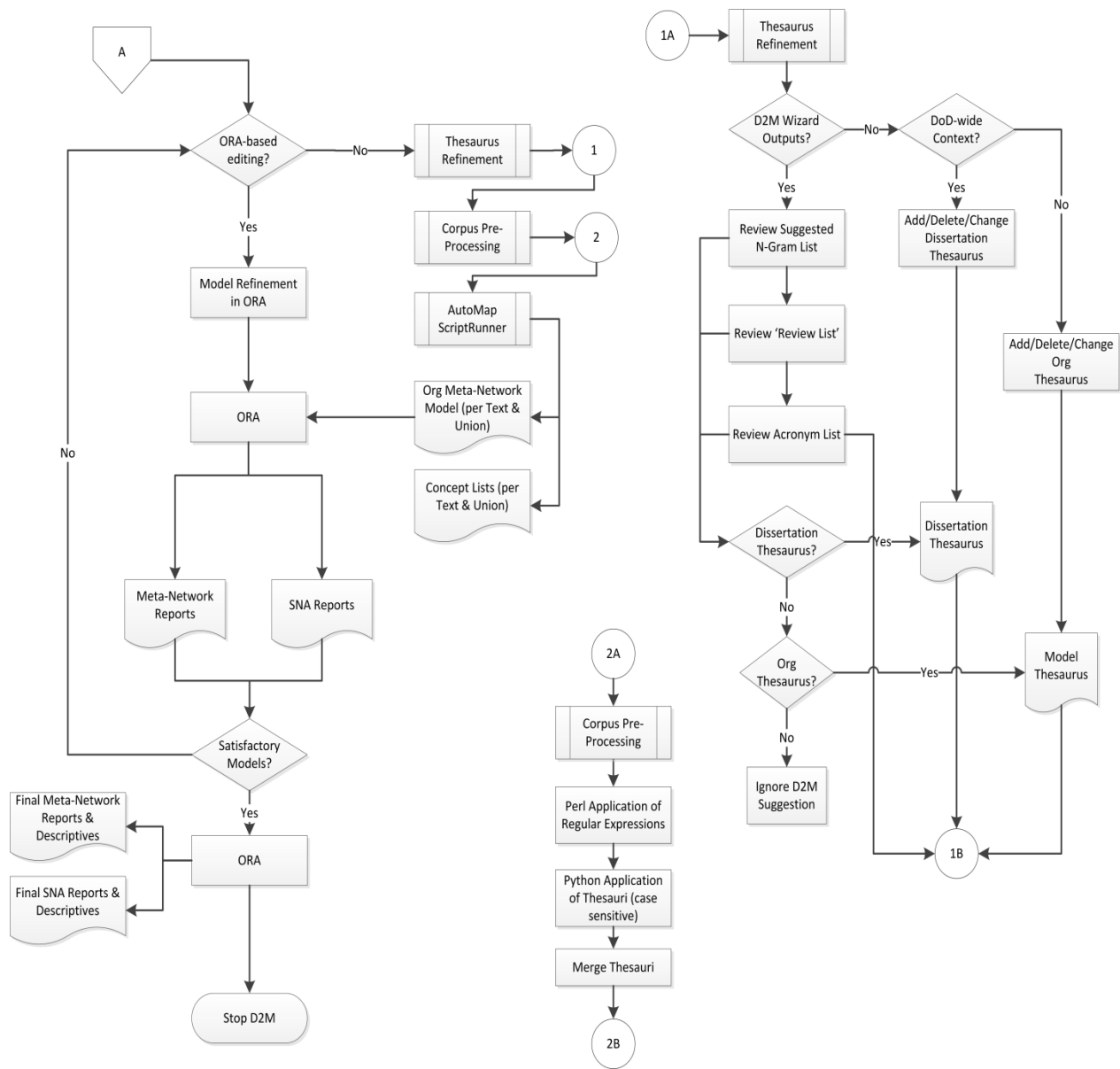


Figure 38: D2M refinement applied to DoD input corpus

Two D2M generated DoD organizational models

The DoD is an organization that expends enormous effort in documenting itself. One of the ways it does this is through the writing and distribution of doctrine documents. DoD includes Joint doctrine in most professional military education courses that have mixed-Service audiences and senior service members. The military departments (e.g., Army, Navy, Air Force) also teach their specific doctrine in professional military education courses, where they place emphasis on the Service rather than Joint operations. The hierarchy of primacy for doctrine within the DoD is Joint followed by Service (i.e., Army, Navy, Air Force, Marine), in accordance with the intent of the Goldwater-Nichols DoD Reorganization Act of 1986 (Baldwin, Picavet, & Reiners, 2009). The Goldwater-Nichols Act emphasized the need and imposed requirements for Services to train and fight as joint entities, and not fiefdoms of expertise and noncooperation.

There are three principle levels of military organizations: strategic, operational, and tactical (which is not in the dissertation). These three levels are identical to what the US military education system often calls the three levels of war. Using two of these levels of war demonstrates the generalizability of the approach from mid-sized organizations to globally dispersed organizations. [Figure 39](#) and [Figure 40](#) are simplified and scoped depictions of the strategic level of command, supported by the descriptions in following sections. [Figure 41](#) is a simplified and scoped depiction of the operational level of command, supported by the descriptions in following sections. I've color coded the diagram with Joint organizations in purple, USAF organizations in blue, civilian components of strategic decision making in red, white, and blue. Mixed colors represent organizations with mixed origins. I also provide a comparison of the descriptive statistics for the D2M Wizard generated models and the iterative refinement generated models. For those interested in replication of the effort, the lists of documents used to build each of these three models are [Appendix 1](#) as well as the bash shell scripts used to collect the documents and transform them into text on my personal web site at http://www.andrew.cmu.edu/user/mlanham/nonpeer.shtml#dissertation_support.

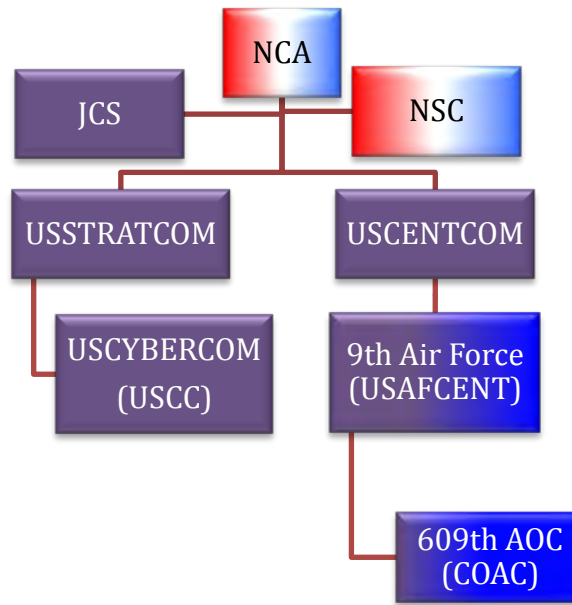


Figure 39: Simplified DoD hierarchy--strategic to operational

National Command Authority to Combatant Commands—the strategic level

The strategic-level organizations I modeled are the National Command Authority ([NCA](#)), US Strategic Command ([USSTRATCOM](#)), US Cyber Command ([USCC](#)), and US Central Command ([USCENTCOM](#)). These are shown in [Figure 40](#). The definition of strategic warfare drives the inclusion of the first three blocks in the figure.

The level of war at which a nation, often as a member of a group of nations, determines national or multinational (alliance or coalition) strategic security objectives and guidance, then develops and uses national resources to achieve those objectives.{Joint Staff J7, 2010 #7253}

The NCA (i.e., “the President and Secretary of Defense together with their duly deputized alternates or successors” (NCA, 2013) supported by the National Security Council ([NSC](#)), the Joint Chiefs of Staff ([JCS](#)), and their respective staffs) is at the top of this level of war. Equally clearly, Strategic Command, to which NCA, through JCS, has assigned long-range military assets (e.g., B2 bombers) and space assets and from which those assets take authoritative orders is part of this level’s model. US Cyber Command, a sub unified joint command of USSTRATCOM, has the responsibility to assure US freedom of action within cyberspace (U.S. Cyber Command Public Affairs, 2010) . I then chose USCENTCOM from the pool of six (6) geographical combatant commands ([GCC](#)) the US operates. This choice derives primarily from the fact that USCENTCOM continues to be engaged in a shooting war with large numbers of US forces, as well as small elements of allied and coalition forces. This engagement often drives

resource allocation within USCENTCOM that might have been different had they not had forces in contact with enemy combatants. The colors coding in the graphic remain the same: purple for the ‘Joint’ units; a blend between Service colors (i.e., blue for US Air Force ([USAF](#)) for ‘Joint’ units predominately from a particular service; and solid colors for units from a particular Service. There are no doctrinal colors for NCA and NSC, so I simply render them in red, white, and blue.

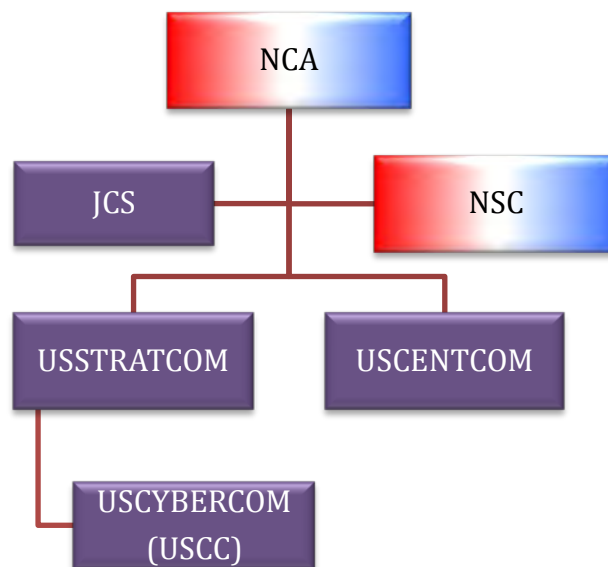


Figure 40: Simplified figure of USG strategic level organizations

COCOM to Numbered Air Force level—the operational level

The operational level of war is the large, and often amorphous, span of military operations and commands between the obviously strategic and the obviously tactical (see also the definition of tactical level of war in the [Alphabetical Definitions](#) (on page [1-7](#)). The official definition is below.

The level of war at which campaigns and major operations are planned, conducted, and sustained to achieve strategic objectives within theaters or other operational areas (Joint Staff J7, 2010j).

In practice, this is the portion of the chain of command that spans from the regional combatant commands ([COCOM](#)) to the first echelon of the tactical level, the division or Service-specific equivalent (e.g., a USAF group, a US Navy battle group, or a US Marine Corps division). For this dissertation, I modeled USCENTCOM and its Numbered Air Force ([NAF](#)) (9th US Air Force). Instead of modeling the 9th AF’s assigned Groups or Wings, I leveraged previous work

(Lanham, Morgan, & Carley, 2011b, 2011e) and modeled its Air Operations Center (609th Air Operations Center), operating as a Combined Air Operations Center ([CAOC](#)). These organizations are shown in [Figure 41](#) below.

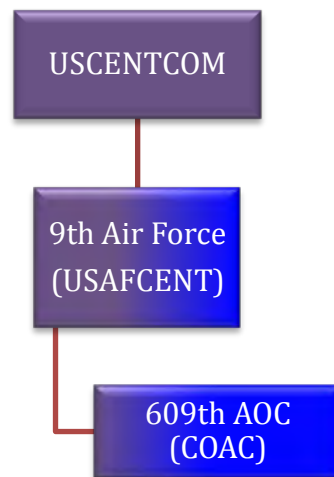


Figure 41: Simplified figure of COCOM and USAF operational level organizations

With the creation of USCYBERCOM, the relationships at this level of command have become increasingly complicated. Complications are from at least two sources. The first is the cyber related direct reporting from tactical elements straight to USCC. The second is the perception, from multiple quarters, that USCC can and should issue cyber related orders directly to tactical elements operating under USCENTCOM's command jurisdiction without de-conflicting their noncyber operational impacts.

Preceding work (Lanham, Morgan, et al., 2011b, 2011e) to this dissertation successfully modeled one portion of a USAF operational level organization called the Air Operations Center ([AOC](#)) and depicted above as [CAOC](#). [Figure 42](#) is an extract from the Air Force Instruction ([AFI](#)) 13-1 (USAF, 2005) that depicts the doctrinal organization of the AOC. [Figure 43](#) depicts the hierarchy of the organization as well as the cross functional area teams as extracted from the AFI during the D2M process.

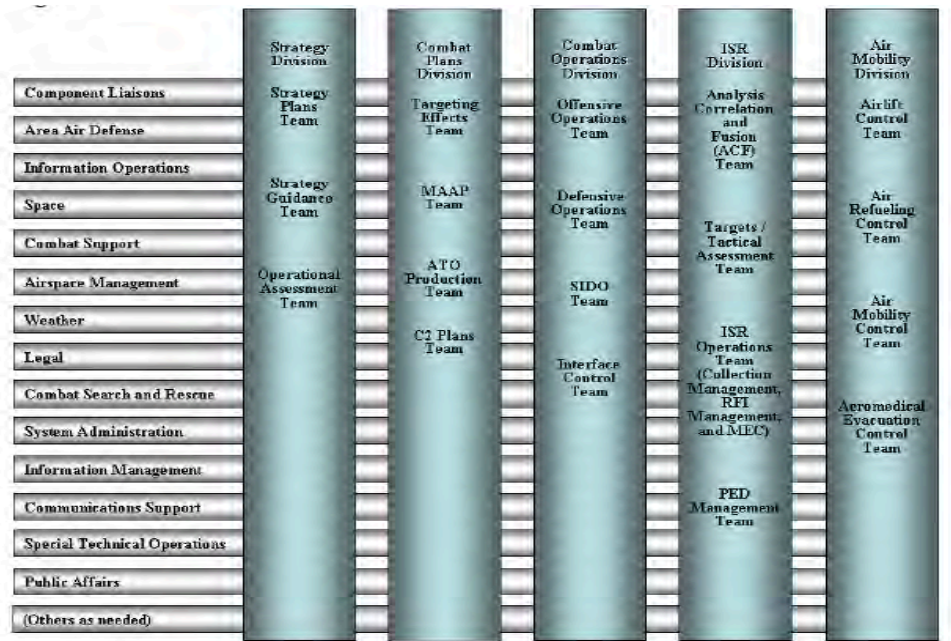


Figure 42: USAF doctrinal air operations center organizational structure

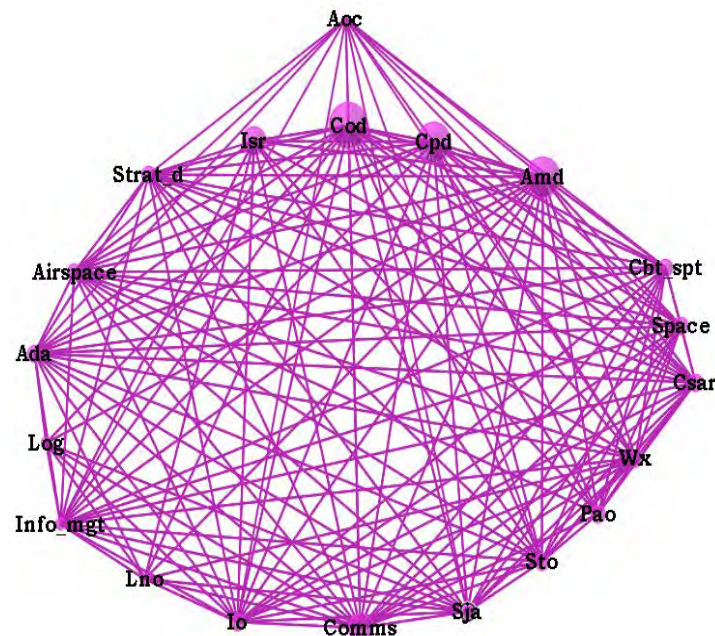


Figure 43: USAF AOC as a text mined model of links and nodes

Inputs of [D2M Wizard](#) and process for each of the two models

There were a total of 139 doctrinal files for the construction of the strategic and operational models.. A tabular summary of the input corpus I used for these models is shown in [Table 9](#) with descriptives of the sizes of each corpus (in megabytes) depicted in [Table 10](#) and [Table 11](#). It is worth noting that there are several open research questions about this selection, as well as any particular sample of any particular corpus when constructing these types of indirect

models. Open questions include: What distribution(s) exist for each of the nine (9) ontologies normalized by MB or KB? Are those distributions domain dependent? Does the sample of documents generate distributions that align with the domain of interest? What are the impacts on processing time (normalized by processor count and available RAM) of the sizes of the input documents? These questions, while interesting, and brief discussions of each are in the [Limitations and Future Work](#) section of the dissertation—they may assist in demonstrating to particular audiences additional facets of model validity as well as offer expectation management with the use of the word ‘rapid’ in the dissertation title.

Table 9: Number of input files per model

Model	Number of Files
Strategic	58
Operational	81
Total	139

Table 10: File sizes descriptives per model/level of war – part 1

	N	Mean Size (MB)	Std. Deviation (MB)	Std. Error (MB)	95% Confidence Interval for Mean
					Lower Bound
Strategic	58	1.7682	1.36599	.17936	1.4090
Operational	81	1.6211	1.27510	.14168	1.3392
Total	139	2.4079	2.50609	.17677	2.0594

Table 11: File sizes (MB) descriptives per model/level of war – part 2

	95% Confidence Interval for Mean	Minimum	Maximum
	Upper Bound		
Strategic	2.1273	.47	7.94
Operational	1.9031	.01	7.94
Total	2.7565	.01	21.27

Outputs of [D2M Wizard](#) and process for each of the generated models

This section has three subsections in it. The outputs of the first iteration of the [D2M Wizard](#), the outputs of the final data-cleaning iteration, and graphical representations of the two models.

Outputs of *D2M Wizard* (cycle 0)

As depicted in [Figure 37](#) (on page [75](#)), the D2M Wizard provides several output files each time a researcher executes it. Two output files of interest are the “suggested ngram” list and the “possible acronym” list. A summary of the sizes of these two output files, per model, is depicted in [Table 12](#) and [Figure 44](#). The variation in the sizes of two files is not a research question of interest, as they are both dependent on the number of input files fed into the [D2M process](#). The information below is illustrative of what a researcher could expect to see if they need to build a research center or project specific thesaurus from scratch by starting with these files. As I had access to the CASOS thesaurus as the basis of the D2M project, I focused my thesaurus generation effort on a DoD-specific model and supplemental per-model level thesauri.

Table 12: Size of D2M wizard generated *suggested ngrams* list and *possible acronyms* list

Model Level	Suggested ngrams	Possible Acronyms
Strategic	174,821	12,273
Operational	207,687	13,192

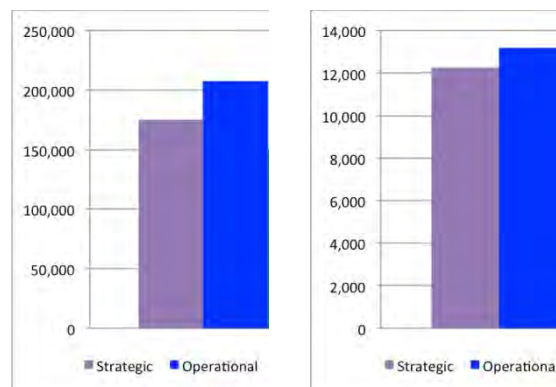


Figure 44: Size of D2M wizard generated ngram list and possible acronym list

Table 13: Quantities of D2M wizard generated concepts as *ngrams* and *singletons* drawn from the union of generated *concept lists*

Model Level	Singletons	N-Grams (multiple words==a single concept)
Strategic	30,205	29,122
Operational	29,821	33,299

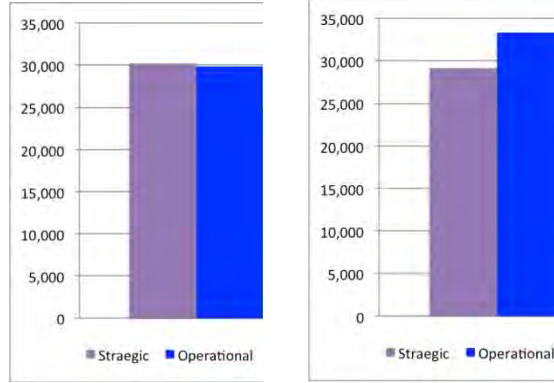


Figure 45: Quantities of D2M wizard generated concepts as *ngram* and *singletons* drawn from the union of generated concept lists

As depicted in [Figure 37](#), other [D2M Wizard](#) output files are the *concept list*, the *finalThesaurus*, and the metanetwork of inter-nodal and intra-nodal links. The *concept list* is a list of D2M identified concepts from the input corpus with the D2M generated suggested ontological category and without any attempt at mapping concepts to other concepts. Fundamentally, it's a direct transcription of the concepts in the corpus reflecting only pre-processing modifications the researcher chooses to execute.

The third and fourth tables below summarize the link and node/entities information, [Table 14](#) and [Table 15](#) respectively, in the first metanetwork created by the D2M Wizard. The D2M Wizard creates links between nodes when those nodes co-occur within a sliding window of words within an input text. This co-occurrence network becomes the metanetwork of the input text with the link weight representing the number of co-occurrences between any two linked nodes. By creating a union of all the metanetworks for each corpus, the D2M Wizard creates a metanetwork from each corpus representing the two models.

Table 14: Metanetwork link descriptives for D2M cycle 0

	Network	Links	Density
Strategic	55	8,760,073	0.00313213
Operational	55	5,983,375	0.00300365

Table 15: Metanetwork entities per ontological category for D2M cycle 0

	raw counts	agent	belief	event	knowledge	location	organization	resource	role	task
Strategic	58,861	3,365	247	83	2,447	489	1,917	2856	281	1,376
% of raw count		5.72%	0.42%	0.14%	4.16%	0.83%	3.26%	4.85%	0.48%	2.34%
Operational	63,120	4,696	36	23	2,434	557	2,660	3630	3	840
% of raw count		7.44%	0.06%	0.04%	3.86%	0.88%	4.21%	5.75%	0.00%	1.33%

The output file *finalThesaurus* serves as a mapping of concepts to concepts, as well as concepts to ontological categories. The *finalThesaurus* file is typically a conglomeration of thesauri that starts with, in this dissertation, the CASOS Standard Thesaurus, mixes in research center thesaurus, domain specific thesaurus, project thesaurus. The precedence of thesauri is reversed, meaning the project thesaurus takes precedence over a domain, over the CASOS standard thesaurus. The information in [Table 16](#) illustrates what a researcher could expect to see after a single iteration of the [D2M process](#) using a research center thesaurus. Of particular note is the column labeled “Unknown” where many automation generated concepts have no ontological category. For each of the models, over 70% of concepts would, ideally, need deletion or an assigned category in the thesaurus. Depending on the corpus and research question(s), other researchers will have different distributions of entities per category per corpus, as well as different sized thesauri. The concepts captured in the D2M process entries in [Table 16](#) are reflective of applying the CASOS thesauri and dissertation thesauri, to the input sets.

Table 16: *Concept list* entities per ontological category for D2M cycle 0

	Raw Counts	#Delete	agent	attribute	belief	event	knowledge	location	organization	resource	role	task	time	Unknown
Strategic	58,861	51	3,365	1,238	247	83	2,447	489	1,917	2,856	281	1,376	250	44,259
% of raw count		0.09%	5.72%	2.10%	0.42%	0.14%	4.16%	0.83%	3.26%	4.85%	0.48%	2.34%	0.42%	75.19%
Operational	63,120	66	4,696	744	36	23	2,434	557	2,660	3,630	3	840	427	47,004
% of raw count		0.10%	7.44%	1.18%	0.06%	0.04%	3.86%	0.88%	4.21%	5.75%	0.00%	1.33%	0.68%	74.47%

Table 17: *finalThesaurus* entities per ontological category D2M cycle 0

	Raw Counts	#Delete	agent	attribute	belief	event	knowledge	location	organization	resource	role	task	time	Blank, None, Unknown
Strategic	518,696	5,520	124,975	5,086	1,246	5,810	76,166	138,107	82,221	43,345	82	8,581	4,572	22,985
% of raw count		1.06%	24.09%	0.98%	0.24%	1.12%	14.68%	26.63%	15.85%	8.36%	0.02%	1.65%	0.88%	4.43%
Operational	541,574	5,581	126,733	6,658	1,245	5,897	80,304	138,440	88,165	46,818	82	8,725	6,276	26,650
% of raw count		1.03%	23.40%	1.23%	0.23%	1.09%	14.83%	25.56%	16.28%	8.64%	0.02%	1.61%	1.16%	4.92%

Final outputs of D2M process

The [D2M process](#) usually requires multiple rounds of cleaning in [ORA™](#), thesaurus addition/modification, evaluation of Key Entities (see also [Equation 12](#) on page 42) reports, and re-execution of D2M Scripts, all of which [Figure 38](#) illustrates. Terminating the cycle of refinement is, at present, a researcher decision based on their question(s) of interest and the types of validation they desire to execute. For this dissertation, and in support of ‘validation in parts,’ I used 20 cycles for the operational model, and 12 cycles for strategic model. Termination conditions I used are shown below.

Table 18: Three (3) terminating conditions for D2M process

1. Key Entity Reports for each node type include no obvious ‘wrong’ entities (e.g., an ‘Agent’ entity in the ‘Resource’ top-10 list) nor entities that could be meaningfully merged.
2. Subreports for Key Entities, for the top 50 entries, included no obvious ‘wrong’ entities nor entities that could be meaningfully merged.
3. Organization models included principal organizational and agent structures typical of military organizations (e.g., Commander, principle staff of A/G -1 through A/G-8, and where appropriate, G8 and G9, as well as AOC-internal structures). Identifiable through tabular data in key entity reports as well as graphical renditions of the metanetworks.

Tabular Summary per Model

The data depicted in [Table 19](#) on page [89](#) reflects the composition of the final versions of each of the three supplemental thesauri the dissertation uses: DoD-wide, Strategic Model, and Operational Model. These supplemental thesauri are deliverables of the dissertation and may reduce the time between starting and conducting useful for future DoD organization modelers. These thesauri are independent of the wizard generated thesauri shown in [Table 17](#)—the entries in [Table 17](#) reflect combination of the CASOS research center’s master thesaurus and the concepts in the three sets. The substantial differences in each of these thesauri are easily understood by recalling that the majority of the DoD-Master thesaurus is from the preceding work modeling and simulating resilient command and control with multiple USAF Air Operations Centers (Lanham, Morgan, et al., 2011b, 2011e). This origin, and the further de-scoping of the dissertation’s operational model, explains the very small model-specific thesauri and the large number of ‘delete’ actions in the operational thesaurus. It was unexpected, though in retrospect not surprising, that the strategic thesaurus is very different. The size of the thesaurus was significantly larger, with each of the ontological categories exhibiting larger changes than

either of the other thesaurus. There is insufficient data across multiple domains and variations within domains to determine if these differences are within the band of normal or not.

[Table 20](#) on [89](#) reflects the composition of the meta-models of each of the models. A brief discussion of the differences between the starting meta-models (see also [Table 15](#) on page [84](#)) and the final models is in order. Each of the metanetworks in cycle-0 had a category of ‘unknown’ that the final models do not contain. The cycle of editing these models and reviewing them for appropriate scope allowed varying levels of reductions in model size, with consequential reductions in processing times within the static assessment as well as eventual simulation. There could be research questions embedded in the apparent difference in the quantity of ‘agents’ in the Strategic corpus compared to the operational corpus. This could reflect an emphasis on the heads of various organizations responsibilities, but it remains an area of future work to determine if there is meaning behind the change in categorical distributions.

[Table 21](#) on page [89](#) provides a very brief view of the sizes and densities of each of these metanetworks. The changes in the nature of each corpus (e.g., its intended audience, orientation to particular levels-of-war) and the varying thesauri created an unexpected variation in the quantities of links and densities. Both models, in cycle-0 had approximately the same density (0.003). I had initially expected that the final densities of the models would align with the final node counts—the highest density would belong to the strategic model with the lowest in the operational model. This remains a question deferred to future work however.

Table 19: Count per ontological category for each of the final thesauri (cycle 12 and higher)

	Raw Counts	#Delete	agent	attribute	belief	event	knowledge	location	organization	resource	role	task	time
DoD-Master	63,586	3,841	3,841	1,719	1,682	1,056	12,333	2,833	10,584	10,056	2,950	12,482	131
% of raw count		6.17%	6.04%	2.70%	2.65%	1.66%	19.40%	4.46%	16.65%	15.81%	4.63%	19.63%	0.21%
Strategic	23,083	3,065	1,196	166	270	492	2,667	1,326	4,219	3,830	426	5,421	5
% of raw count		13.28%	5.18%	0.72%	1.17%	2.13%	11.55%	5.74%	18.28%	16.59%	1.85%	23.48%	0.02%
Operational	1,611	1,525	4	-	-	-	26	2	46	5	1	2	-
% of raw count		94.66%	0.25%	-	-	-	1.61%	0.12%	2.86%	0.31%	0.06%	0.12%	-

Table 20: Metanetwork entities per ontological category (cycle 12 and higher)

	Raw Counts	agent	belief	event	knowledge	location	organization	resource	role	Task
Strategic	25,190	3,308	469	317	4,216	1,379	3,696	5,456	694	5,619
% of raw count		13.13	1.86	1.26%	16.74%	5.47	14.67%	21.66%	2.76%	22.31%
Operational	17,635	1,481	443	168	4,195	850	4,142	2,358	788	3,210
% of raw count		8.40%	2.51%	0.95%	23.79%	4.82%	23.49%	13.37%	4.47%	18.20%

Table 21: Metanetwork descriptives (cycle 12 and higher)

	networks	links	density
Strategic	45	1,695,229	0.00534342
Operational	45	1,546,983	0.00994922

Table 22: Counts of N-grams, singletons, acronyms, nonacronyms (cycle 12 and higher)

Element	Quantity	Percentage
N-grams	42,920	62.7%
Singletons	25,563	37.3
Acronyms	4,664	6.8%
Non-Acronyms	63,819	93.2%

[Table 22](#) allows a comparison between the cycle-0 lists of possible ngrams and acronyms to the contents of the final DoD-Master Thesaurus. The final thesaurus has more ngrams than cycle-0 estimated, and fewer acronyms. The cause(s) of the variation is not clear, though I suspect the acronym-to-ngram conversion in the thesaurus is partly responsible—I deliberately converted many acronyms to their ngrams, as well as included their ngrams as part of the thesaurus. Nor is it entirely clear if the cause(s) of the variation are relevant to the research question at hand.

[Table 23](#) depicts a component of the output model that the D2M process is not yet capable of generating. The specific nature of this research question requires the ability to differentiate agents and resources that a contested cyber environment can affect. There is no direct mechanism in the text-mining process to differentiate such agents and resources. Instead, through a completely manual process, I reviewed the lists of agents and resources for the various models and created ‘attributes’ that would allow me to differentiate IT agents from non-IT agents. Examples of IT agents are computer systems that generate or receive electronic messages, with or without direct human intervention. IT agents also typically perform some level of storage and processing on those messages as well as support habitual interaction by humans in the performance of their human-tasks. Examples of such systems include: Email, Blue Force Tracker, web-portals, databases, chat servers, and other such systems. A set of encoding heuristics is shown in [Table 61](#) for continued use or clarification.

Clearly, many IT systems susceptible to contested cyber environments do not fit into that somewhat amorphously defined category of IT agents above. As a simplification mechanism, I have an additional category that I have labeled IT resources. These are information technology dependent or enabled capabilities that I do not consider message generating or passing. Nor do I consider them as storing or manipulating messages—exclusive of data caching and temporary storage such as a router and its routing tables. There is some level of risk in how and where I drew boundaries for these two groups, as neither label adequately expresses distinctions or multi-purposed systems—are radars resources and their processing units IT agents or is the entire radar system (e.g., emitter, receiver, processing and communications units) an IT agent? The necessity of applying arbitrary selection criteria for binning these systems and systems-of-systems is a reflection of the gaps in the research space I discuss in the related literature. It may be infeasible to create a

contested cyber environment against radar emitters and receivers (ignoring the debates about whether electronic jamming or spoofing, electronic warfare is a form of cyber operations), though should an adversary act against processing or communications components, it is feasible to create effects through the loss of confidentiality, integrity, or availability.

The distribution of IT agents and IT resources within the models, as well as the master attributes list in [Table 23](#) does provoke some thoughts: of specifically named and mentioned agents in the sets, over 20% are named or otherwise specific IT systems. This substantial fraction of agents is in line with the quantity of popular media stories and concerns by USG officials that the DoD is susceptible to contested cyber environments. Clearly, simple mentions of systems in doctrine and other documents does not necessarily connote their place or importance within organizations' ability to execute their missions—it does however provide one more quantitative, not subjective, data point in mission assurance assessments. What I found somewhat more surprising is the smaller percentage of resources that fell into the IT resource bin. At just over 5% of the total number of resources, is there room for making a, possibly naive, assertion that such a small percentage of assets should never be cause for concerns about 'Cyber Pearl Harbors' and 'existential threats?' There is certainly room for such an assertion, but like IT agents, such infrequent references in doctrine may not indicate their actual importance within organizations. The inability of simple counting of references to establish importance to organizations is yet another reflection of the gaps in existing research.

Table 23: IT related agents and resources in all three generated models (cycle 12 and higher)

	Agents (IT & Non-IT)	IT agents	Resources (IT & Non-IT)	IT resources
DoD-Master Attributes List	3,303	852	10,056	578
% of node type		22.18%		5.75%
Strategic Model	3,303	242	5451	161
% of node type		7.33%		2.95%
Operational Model	1,386	373	2,342	124
% of node type		27.21%		5.29%

Moving from tabular summary to one of the strengths of ORA™ as a network analytics tool, I will now review the terminating Key Entities reports for each of the three models.

Final Key Entities Report – Operational

The Key Agents visualization for the operational model, with the agent node set remaining the aggregation of human agents and IT systems identified in the source documents is in [Figure 46](#). The figure shows ‘Commander’ ranks in the top three in 90% of agent-related measures with the more specific ‘Combined Joint Force Air Component Commander’ (CJFACC) being the next highest ranked agent, tied with ‘adversary,’ at 56%. Unsurprisingly, Joint and Air Force doctrinal documents place great emphasis on the commander, and his/her place in the organization.

To further assess the validity of the top-three agent recurring report, I expanded the visualization to those agents that consistently appear in the top 20 of their respective measures. This expanded view is shown in [Figure 47](#) where the nonspecific agent ‘Commander’ remains in the top most position, with the CJFACC now tied. There remains some ambiguity in the source text about the Joint Staff—this technique is not yet capable of differentiate whether a given reference is to the Joint Staff supporting the Joint Chiefs of Staff in Washington, D.C., or the staff of a joint command. Of potential note is the absence of a specific agent, other than commanders, usually associated with the cyber domain. There is however, a number of IT systems in this expanded view, to include the generalized common operating picture (COP), the [ISR](#) Tracking System, and the generic ‘information system.’

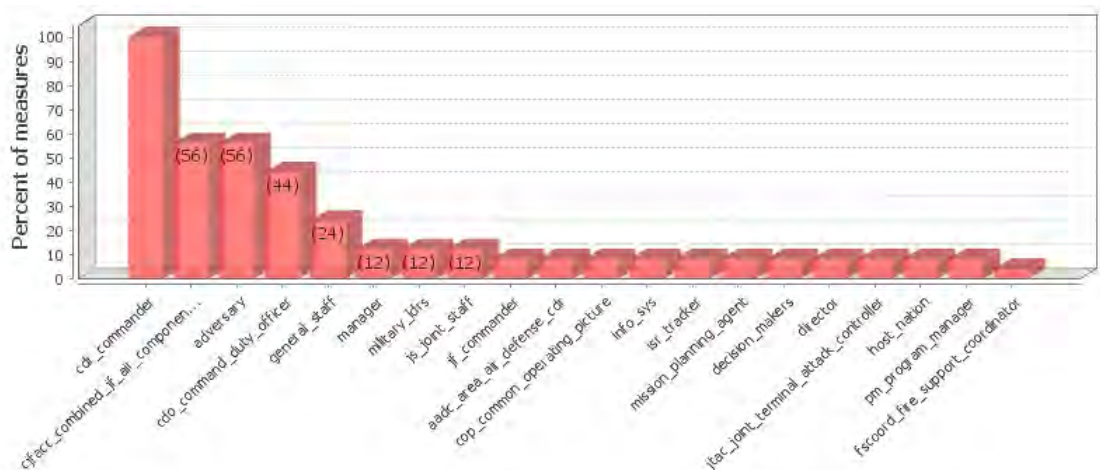


Figure 46: Recurring top ranked agents (top 3), operational model

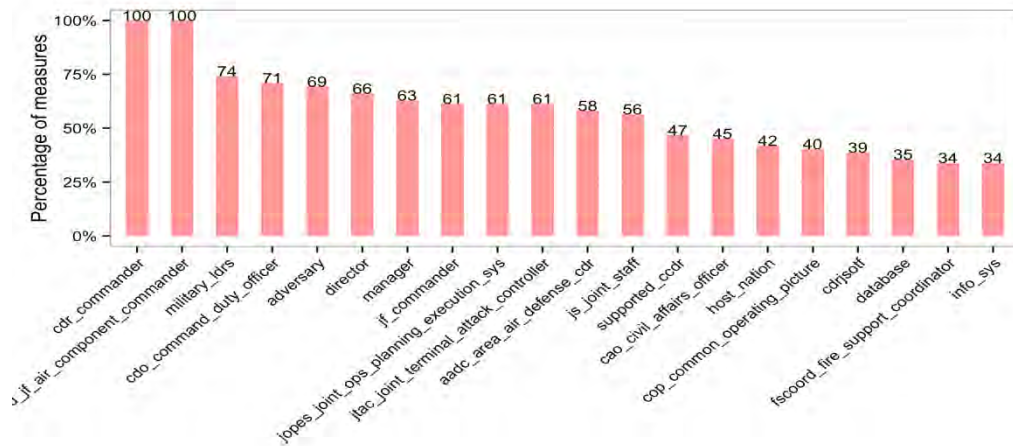


Figure 47: Recurring top ranked agents (top 20), operational model

It is necessary to disaggregate the IT agents from the agent node class to gain a better understanding of the relative importance of the human and IT agents within the metanetwork. This disaggregation allows for a finer grained understanding of the structural characters of two different agent types. The disaggregated human recurring agents visualization is below in [Figure 48](#). In it, the corpus clearly reveals a high level of emphasis (and high variability within measures) on commanders and various specific organizational leaders. The paucity of the agents displayed is indicative of the variability of the human agents' rankings within each measure.

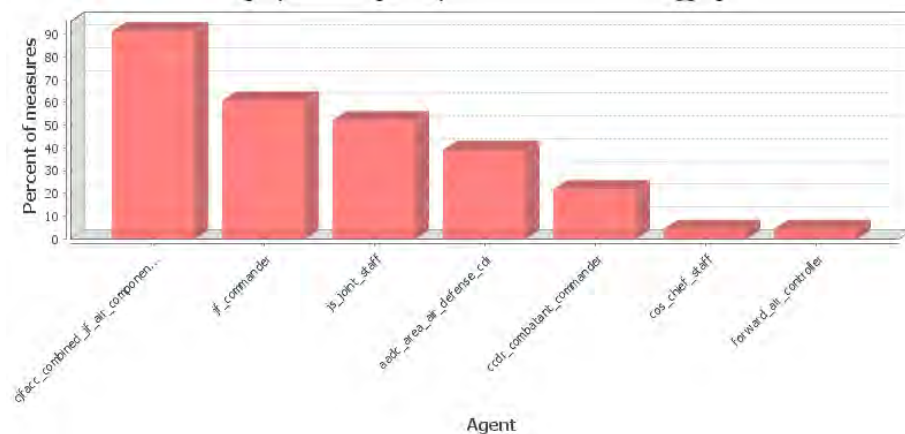


Figure 48: Recurring top ranked human agents (top 3), operation model

To overcome the small number of agents revealed above, I again expanded the window of recurrence to the top 20 finishers in each measure. With this expanded view, in [Figure 49](#), the human agent population continues its lack of cyber oriented agents and

remains focused on Air Force operations. It did expand to include a number of other specific military leaders at various levels. One feasible interpretation of this emphasis on leadership is the Air Force’s doctrine places the emphasis of mission assurance on commanders and military leaders and not cyber specific agents or roles.

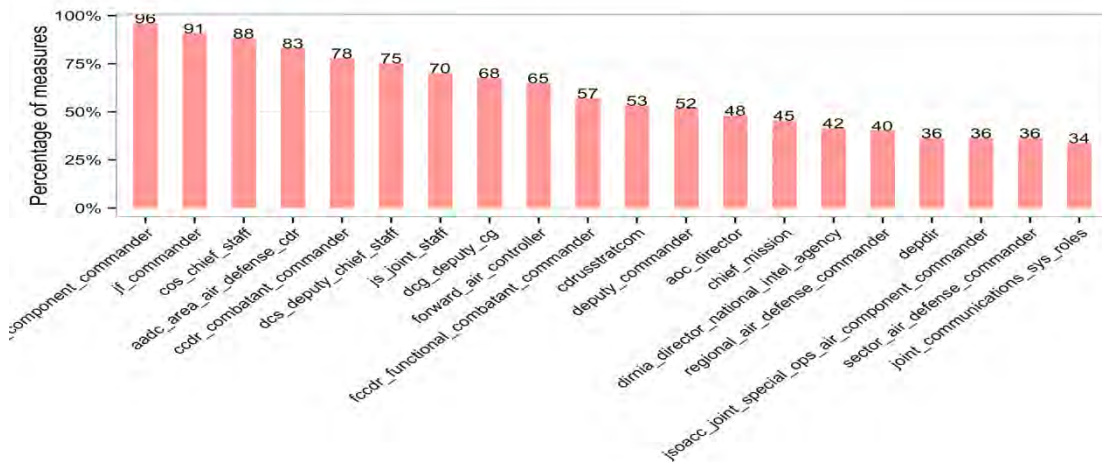


Figure 49: Recurring top ranked human agents (top 20), operational model

For the disaggregated IT agents population, when limited to the top 3 finishers per measure, the information revealed in [Figure 50](#), demonstrates variability among the doctrine documents about which IT systems are important enough to be specifically mentioned. The Global Command and Control System ([GCCS](#)), in all its Service-specific incarnations, is the most frequently mentioned IT system, but even then is only in the top three of measures 50% of the time.

Extending the window of analysis to the IT agents that are in the top 20 of each measure, reveals a piece of information that I had previously thought of as anecdotal only—units rely on internet relay chat ([IRC](#)) much more casual observers might believe. Variability is still fairly high, though GCCS is now joined by the generic COP, the Joint Operations Planning and Execution System ([JOPES](#)), as well as the theater battle management core system ([TBMCS](#)) as frequently mentioned IT systems. This report provides evidence that SME-based assessments of the importance of TBMCS, JOPES, and GCCS are supported with quantitative analysis.

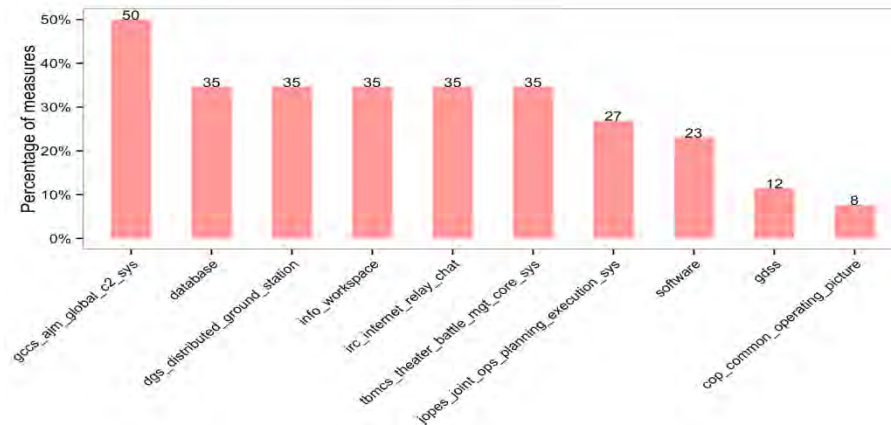


Figure 50: Recurring top tanked IT agents (top 3), operational model

At the organization level, Joint and USAF doctrine are highly variable for the organizations that are consistently and frequently mentioned. This is shown in [Figure 52](#) where only the generic organization of ‘staff’ rises to the 80% mark for consistent importance in network measures. Not surprising in their presence, though their low values remain at odds with professional experience, are the staff divisions for Intelligence and Operations. I had expected these organizations to be prominent in this kind of report and graph. A possible source for the discrepancy is the common mental models of authors—if they all simply ‘know’ that operations and intelligence divisions are important, they do not write such apparently self-evident facts. It’s unclear that commanders at the operational level of war would necessarily be surprised—if there was such a common reaction, the discrepancy could help Services adjust their writing styles.

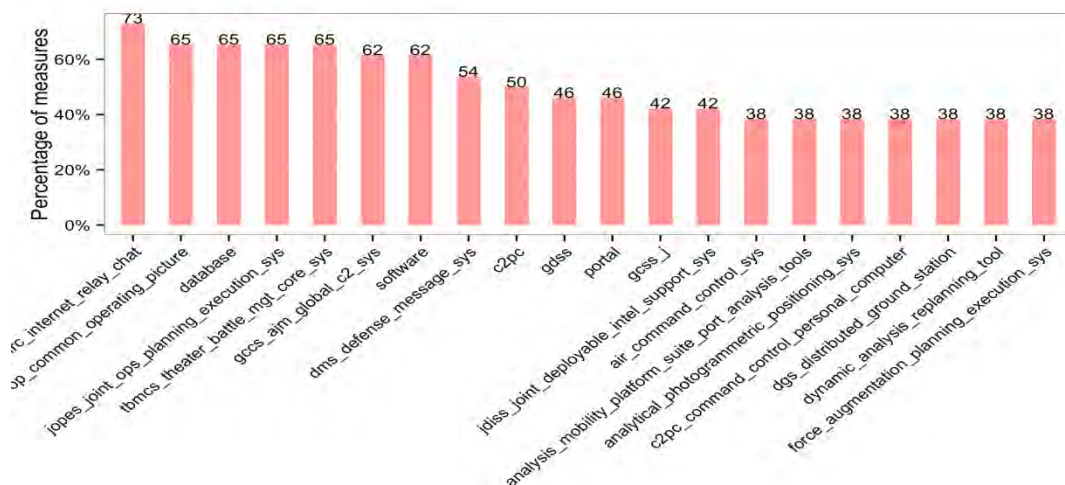


Figure 51: Recurring top ranked IT agents (top 20), operational model

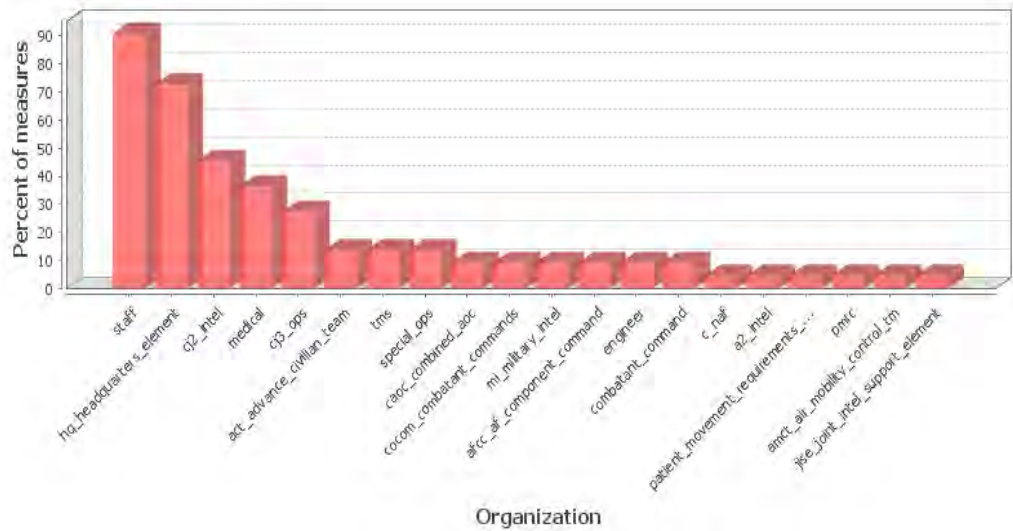


Figure 52: Recurring top ranked organizations (top 3), operational model

Expanding the threshold for visualization from the top 3 recurring organizations to the top 20, [Figure 53](#) below, allows us to see the results does not appreciably change, though the number and types of units certainly does. At this threshold, the top entries do not change in their inclusion or relative order with the exception of the operations divisions. There is certainly ambiguity over which level of joint staff operations this entity refers to—National J3, COCOM level J3, Joint Task Force J3, or Combined Joint Staff J3. The absence of the logistics community in this model is likely more a reflection of the corpus selection than a lack of institutional emphasis on logistics at the tactical levels. It is extremely unlikely that the Air Force is cavalier to the importance of their logistics tail to their ability to conduct operations.

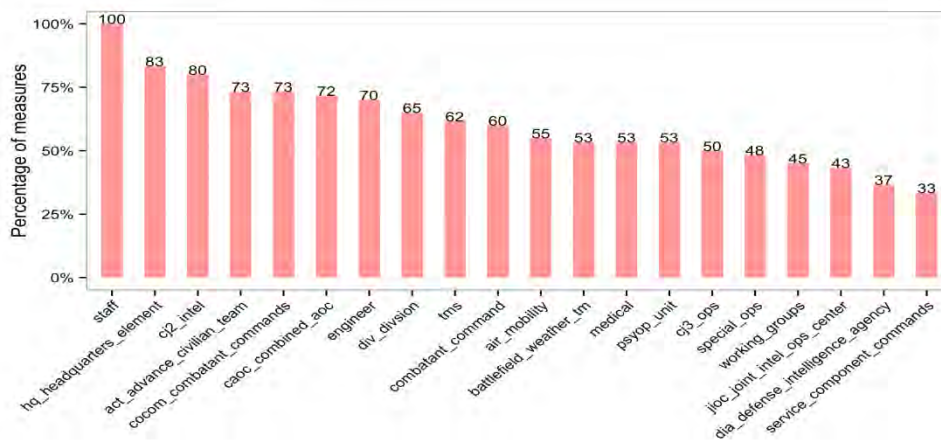


Figure 53: Recurring top ranked organizations (top 20), operational model

The Operational Model Resources captured by the D2M process, below, and the thesauri I applied yield only a four (4) entities that doctrine consistently cross the 25% threshold. Like the tactical model, the aggregation of IT resource and non-IT resource in this report is not terribly illuminating.

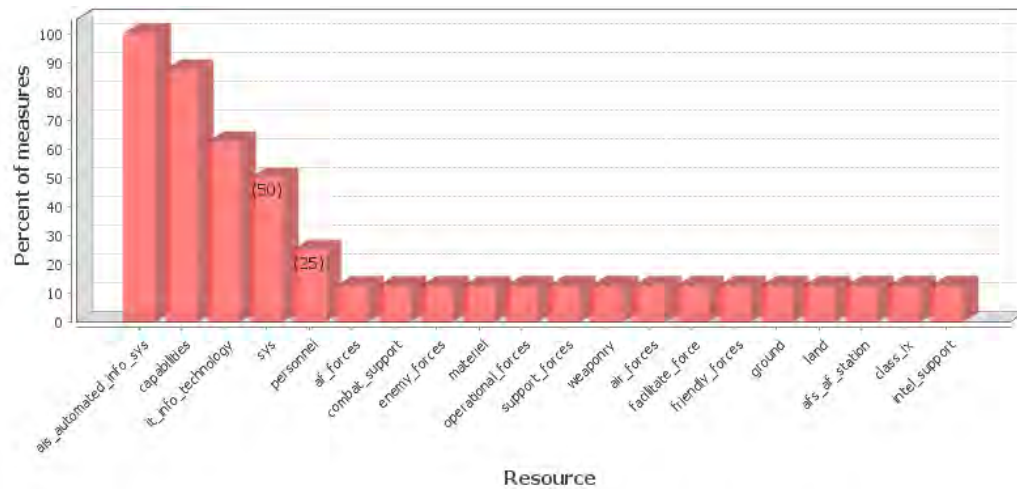


Figure 54: Recurring top ranked resources (top 3), operational model

Expanding the window of analysis to the resources that appear in the top 20 of these measures, [Figure 55](#), does not yield any more coherent presentation of resources that are specific enough to address and important enough to have organizations dedicate resources to improving their resilience. It is gratifying to see that networks and IT, both in generic incarnations, are in this view of the data, though lower than professional experience would lead me to expect.

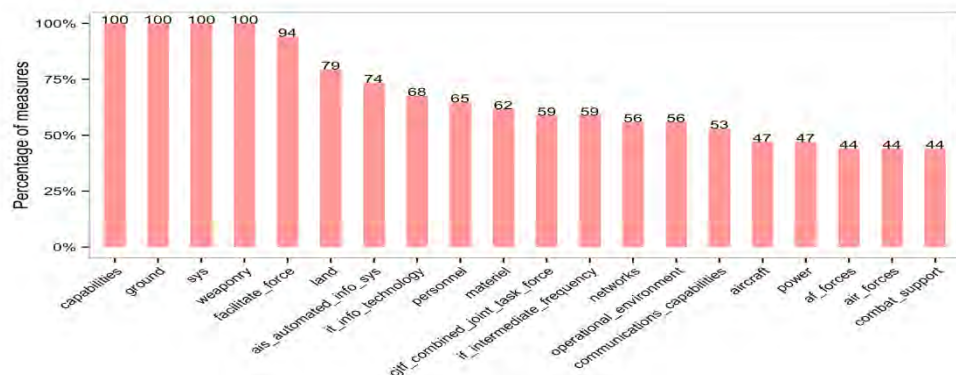


Figure 55: Recurring top ranked resources (top 20), operational model

When disaggregating IT resources from non-IT resources, the resource picture does not become more meaningfully clear, though a review remains in order. Below, [Figure 56](#)

depicts that there are only three (3) highly generic resources that rise to the top 3 even 10% of the time. The generalized resources of capabilities, systems, and personnel are insufficiently precise to drive assessments of mission assurance. This insufficiency is, possibly, a selection error. The result may be a function of the texts that comprise the evaluated corpus—a corpus more precisely aligned with a specific organization may generate more meaningful results. Before making further judgments on the usefulness of this disaggregation and report, it's time to review the top 20 results of each measure and the disaggregated IT resources generated in the D2M process.

In [Figure 57](#), the same generic resources are at the top of the list, revealing that they are in the top 20 of all the resource-related measures. This report and analysis though is equally nonrevelatory as the previous report. The doctrine, as the source of the data, is insufficiently verbose in the resources listed to support primary decisions about named resource importance. However, a metanetwork ontology's strength is that one segment of a model may not have direct measurable significance, but that segment still exists within the structure of the overall evaluated model. This presence supports the face validity of the model, and potentially increases the acceptability of results from other portions of the structure and model. In other words, importance to the network may very well be in the positioning within the multi-node system, not simply existence of a single node class.

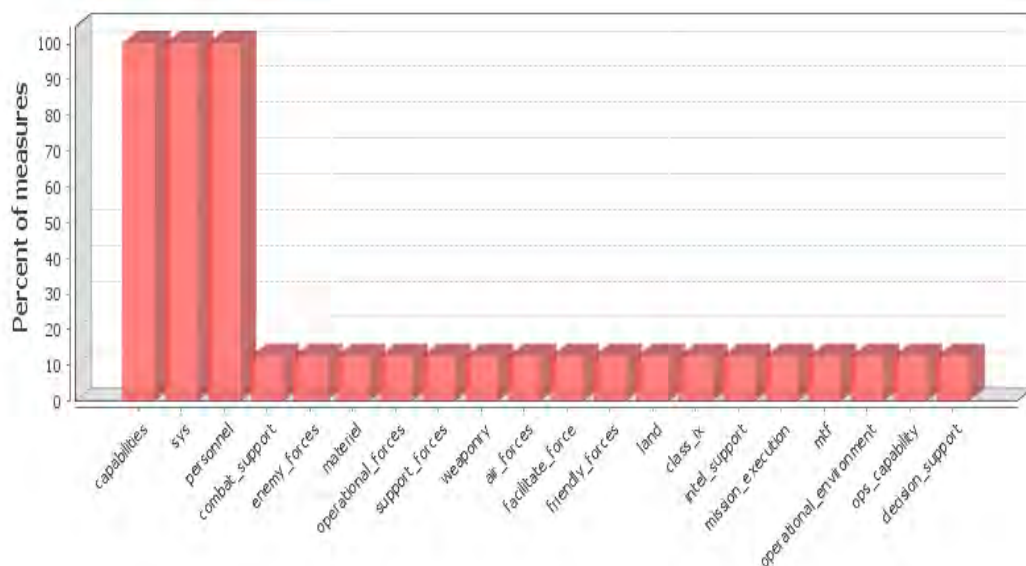


Figure 56: Recurring top tanked Non-IT resources (top 3), operational model

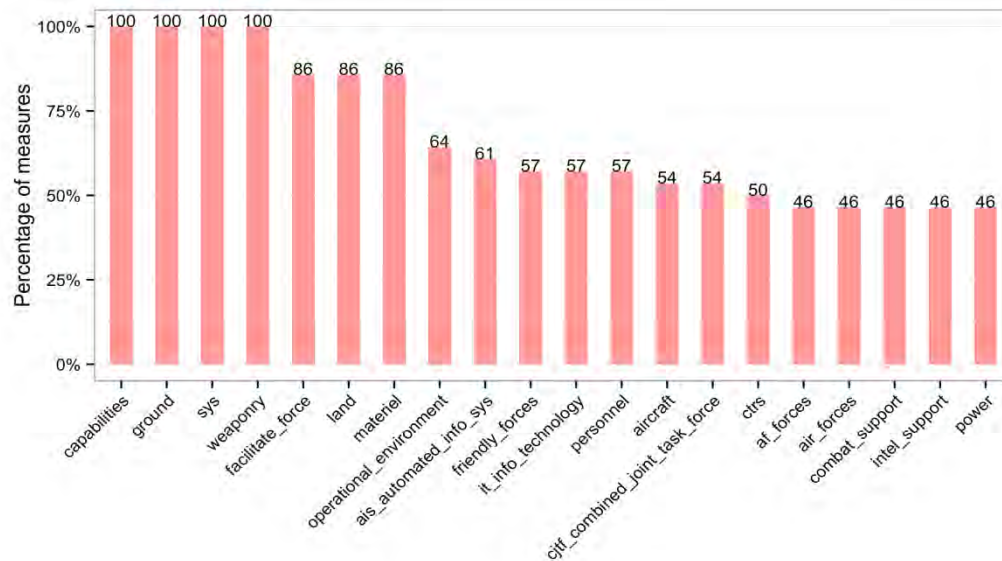


Figure 57: Recurring top ranked Non-IT resources (top 20), operational model

The IT resources graphs, in contrast to the non-IT resources graphs, reveal entities that are recognizable and reasonable to Combatant Command and US Air Force cyber familiar and aware personnel. [Figure 58](#) reflects the importance that popular media places on communications capabilities (of all types with no specificity) as well as networks (generally) and computer networks. There is some ambiguity whether ‘networks’ and ‘computer_networks’ refer to the same concept or if there was some meaningful contextual difference in the corpus. Given previous reports on the relative importance of the intelligence divisions of this level of warfare, it is gratifying to discern the intelligence network (JWICS) being present in the report as well. It is interesting to note that the named unclassified and secret networks (NIPRNet and SIPRNet) are not apparent while JWICS is present. The tactical model also reflected this absence of NIPRNet and SIPRNet.

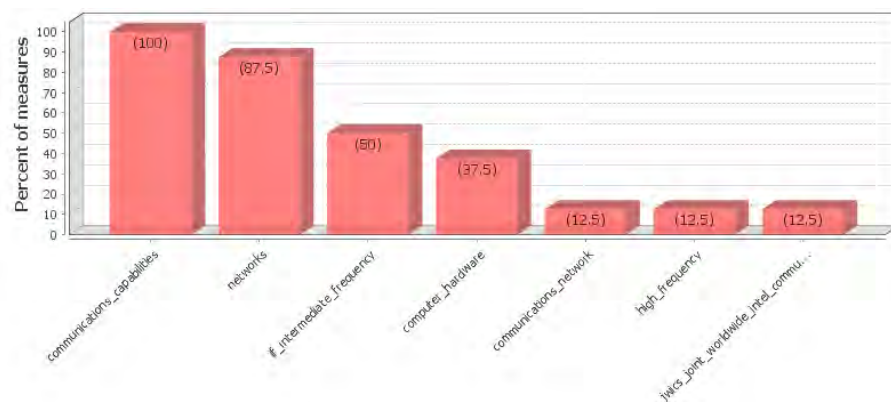


Figure 58: Recurring top ranked IT resources (top 3), operational model

Expanding the analysis window to the top 20 finishers in each resource related measure generates [Figure 59](#). In this chart the generic communications capabilities remain high in the report, and JWICS rises even higher. The World Wide Web is a relabeling of NIPRNet (not technically accurate but a reasonable abstraction) and has near parity with JWICS in this view. Interestingly, a specific-to-coalition environments network (e.g., Combined Enterprise Regional Information Exchange ([CENTRIX](#))) appears in this view, which corresponds to the national trend of operating in coalition environments. There is also a more apparent importance of satellite based capabilities such as Global Positioning System (GPS), communications, and the generic ‘space_capabilities’—a frequent euphemism for classified capabilities).

This operational-level section has demonstrated that the second of the three stopping conditions listed in [Table 18](#) is met. Later in this chapter, we will see the evidence of meeting the third stopping condition for the operational model.

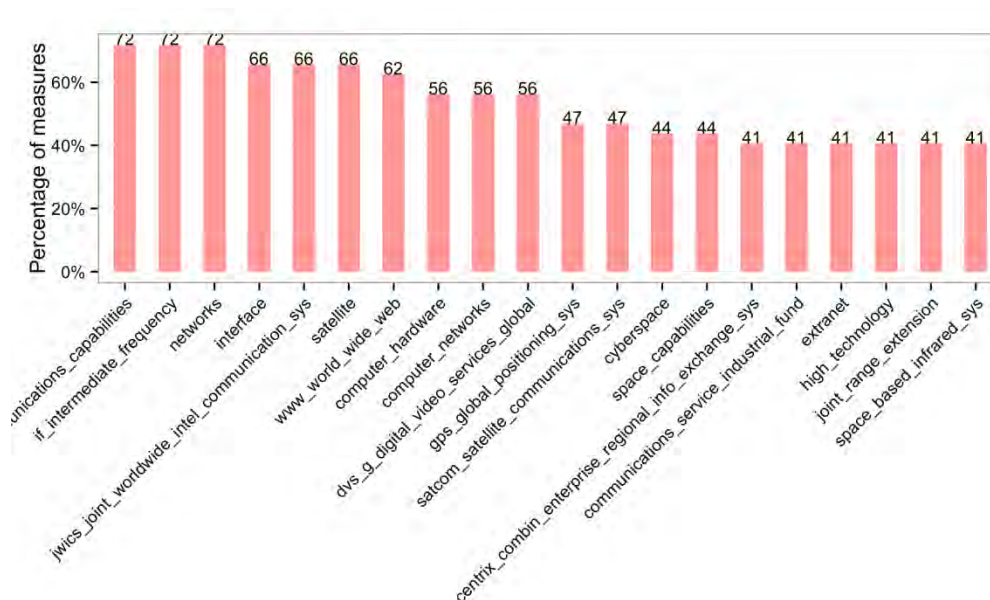


Figure 59: Recurring top ranked IT resources (top 20), operational model

Final Key Entities Report – Strategic

This section is similar to the previous operational model just discussed, the Key Entities Reports review of D2M output for the Operational models. It provides a snapshot of the complete quantitative and visual representation of key entities for interesting node sets. I,

again, provide the complete key entities reports (all 238 pages) on my home page at http://www.andrew.cmu.edu/user/mlanham/nonpeer.shtml#dissertation_support.

The Key Agents visualization for the strategic model, with the agent node set remaining the aggregation of human agents and IT systems identified in the source documents, is in [Figure 60](#). The figure shows ‘CDR-Commander,’ ‘Combatant Commander’ (Combatant Command Commander), and ‘SECDEF’ (Secretary of Defense) rank in the top 3 in 100%, 86% and 84%, respectively, in twenty-nine (29) different measures. The generic ‘info_sys’ and [JOPES](#) (Joint Operational Planning and Execution System) are the only two IT specific agents that make it into this summary of the measures. Like the other two models, it is not surprising that Joint doctrinal documents place great emphasis on commanders in general while specifically calling out Combatant Command Commanders, and the Secretary of Defense. In the US military chain of command, the [SECDEF](#) is second only to the President for civilian leadership. Unsurprisingly, at least in the aggregated collection of human and IT agents, named and specific IT systems are not frequently in the doctrine in the top 3 places of the various measures. One explanation of this could be it reduces the probability of needing to republish doctrine for each new technology change. Another plausible—and not mutually exclusive—explanation is that doctrine is supposed to be a guideline and framework—not a specified collection of how and when to use what tools to accomplish tasks. There were several surprising aspects to the results: the low ranking of the CJCS ranked, the almost complete absence of supporting staff positions, and the missing National Security Council given its role in US military operations.

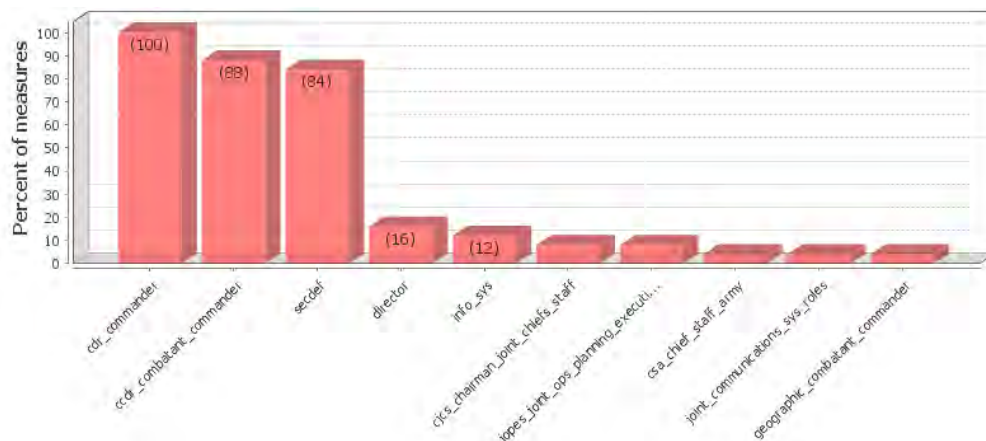


Figure 60: Recurring top ranked agents (top 3), strategic model

Using the same process as the other two models, the expanded visualization of those agents that consistently appear in the top 20 of their respective measures is shown in [Figure 61](#). In this expanded view, the top three agents are identical, though their relative position has changed with the SECDEF rising to the second place. The Geographic Combatant Commanders have risen to the 3rd place in this chart, revealing there is ambiguity in doctrine when authors refer to Combatant Commanders—variants include Combatant Commanders, the Geographical Combatant Commanders, or the Functional Combatant Commanders, or some combination. Also in this view, we begin to see the presence of IT specific systems, though their labels remain generalized (e.g., info_sys, databases, and common operating picture) with one specifically named system: Global Air Mobility Support System ([GAMES](#)).

Disaggregating the IT agents from the human agents yields another example of differentiating the relative importance of the two agent types. The disaggregated recurring human agents visualization is below in [Figure 62](#). The disparity between the three (3) most important agents and the remainder was not expected and is not reflective of what professional experience would have suggested.

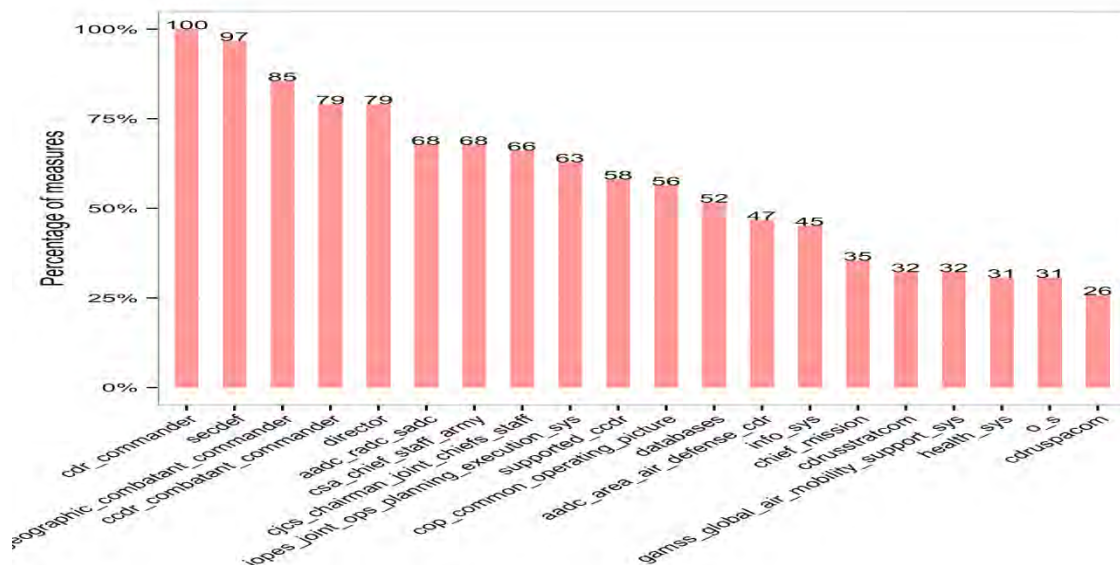


Figure 61: Recurring top ranked Agents (top 20), strategic model

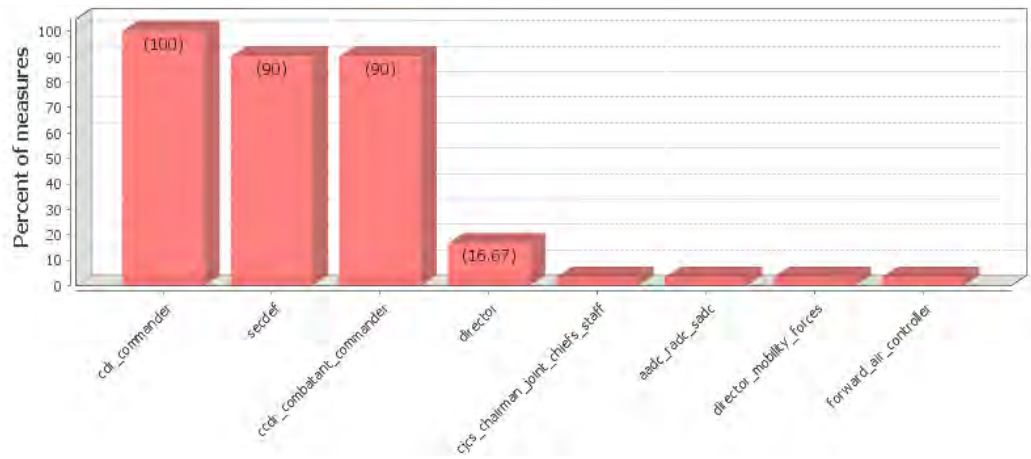


Figure 62: Recurring top ranked Human Agents (top 3), strategic model

For further exploration of the top ranked human agents, I again expanded the window of recurrence to the top 20 finishers in each measure. With this expanded view, in [Figure 63](#), the human agent population has a much broader swath of responsibilities than the generic ‘commander’, the Secretary of Defense ([SECDEF](#)), and the Combatant Commanders. With this expanded view, we start seeing the inter-relatedness of the logistics community (e.g., [USTRANSCOM](#)), the intelligence community ([IC](#)) in the form of the Director of National Intelligence ([DNI](#)), the individual military departments and the component commands those departments furnish. Though it may have been reasonable to prune the model to reflect only those organizations in [Figure 40](#), I decided that for the initial stopping point of face validity to allow the intermingled data/entities to remain where the corpus placed them.

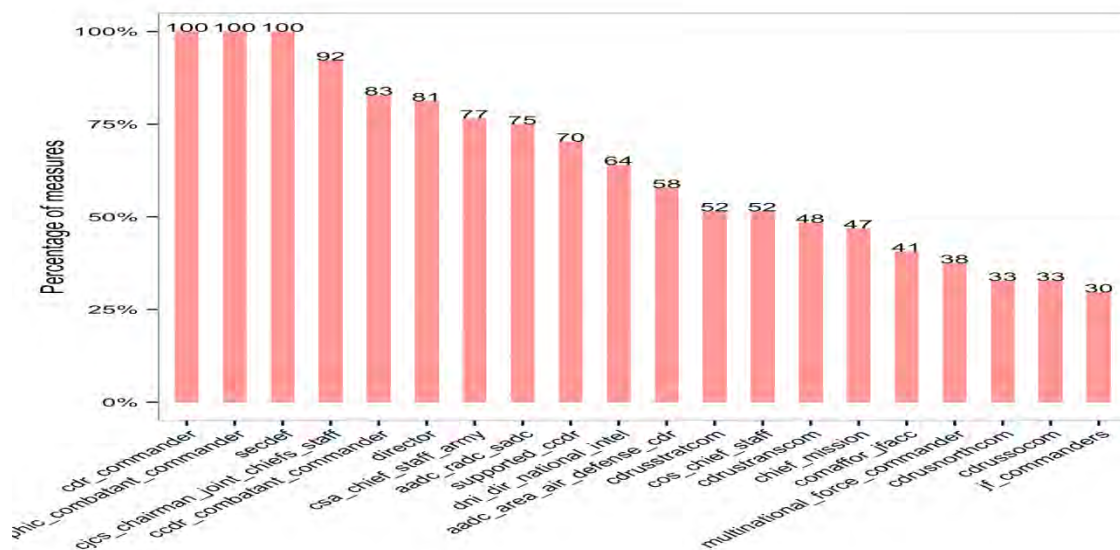


Figure 63: Recurring top ranked Human Agents (top 20), strategic model

For the disaggregated IT agents population, the information revealed in [Figure 64](#) demonstrates the near universal prominence in doctrine held by JOPES. Generic databases are a near second with all other specific IT agents in the top three of the measures 30% of the time or less. With such variability, the continued expansion of the analysis window to the top twenty (20) finishers in each measure remains apropos.

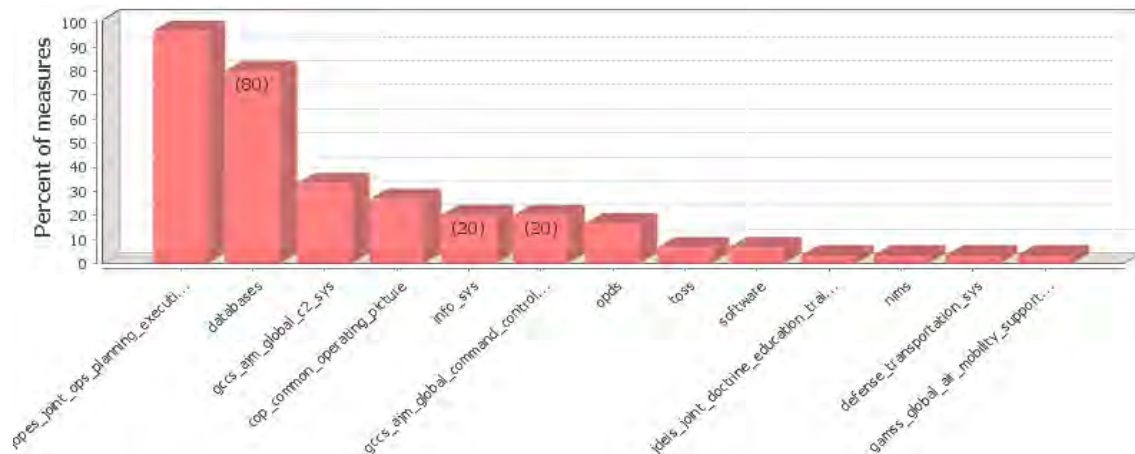


Figure 64: Recurring top ranked IT agents (top 3), strategic model

[Figure 65](#) reveals that at this level of granularity, there is much less variability between the named IT systems. The number of supporting interests has also grown from those whose primary consumers are ‘commanders’ to multiple supporting interests and elements (e.g., intelligence, supply operations, and provide/operate/maintain network/telecommunication networks).

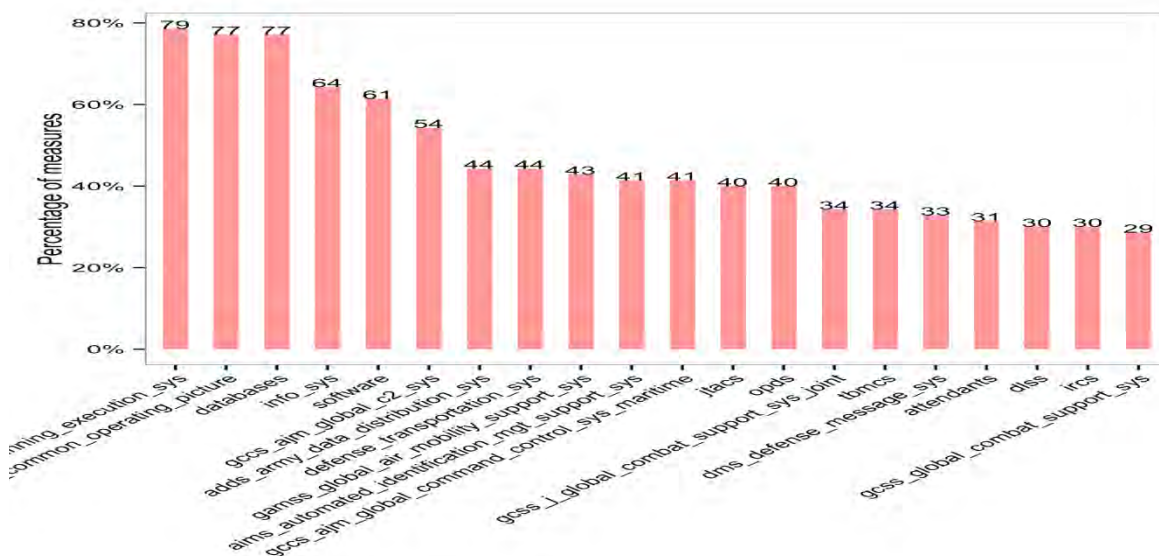


Figure 65: Recurring top ranked IT agents (top 20), strategic model

At the organization level, the strategic model reveals that doctrine writers have broadened their scope of interest to include numerous organizations inside the Department of Defense as well as other governmental agencies ([OGA](#)), as shown in [Figure 66](#). The top ranked organizations form the top tier of the nation’s war fighting commands—the combatant commands, their respective service component commands, and their respective higher headquarters. The rankings of the other displayed organizations, at less than 10% of measures, remain too varied to do more than speculate about meaning or causation.

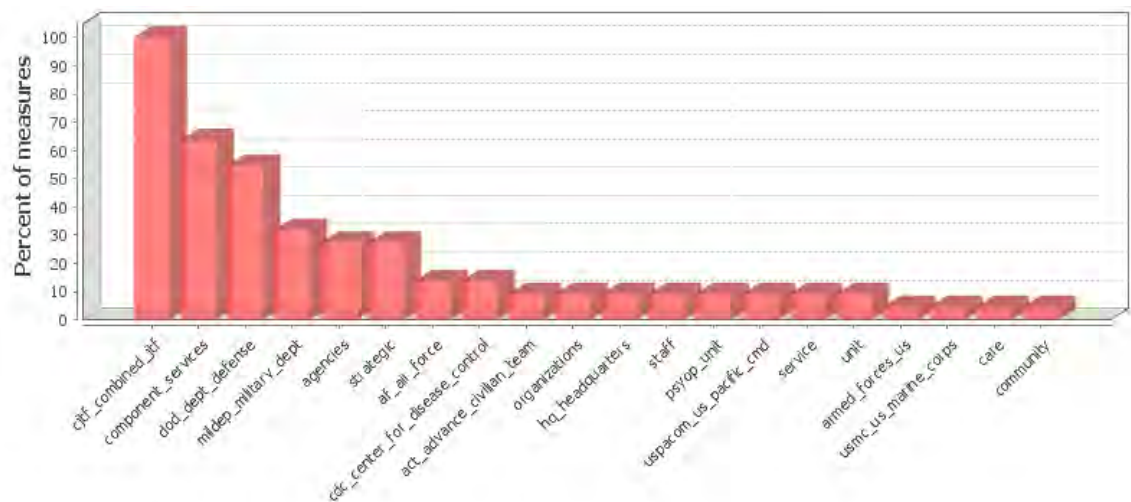


Figure 66:: Recurring top ranked Recurring top ranked organizations (top 3), strategic model

Expanding the threshold for visualization from the top 3 recurring organizations to the top 20 allows us to see the robustness of the model. The variability in depicted results is smaller than previously as well as reflecting a wider variety of organizations that strategic doctrine writers frequently mention. This result is reflective of the actual complexity of organizations that come together to wage our nation’s wars: its more than infantry, tanks, and airplanes fighting in and over muddy fields. From the D2M process, the model includes not only the principal strategic military formations, but also elements of other government entities (e.g., [CDC](#)), Field Agencies and Agencies, and the ubiquitous Special Operations Forces ([SOF](#)).

The Strategic Model’s resources, [Figure 68](#) below, depict several nonspecific resources but most interestingly, one very specific IT based resource: Joint World Wide Intelligence Communications System ([JPG_joint_planning_group](#)

[JWICS](#)). The consistently and prominent presence of this IT resource is indicative of the value of both intelligence at the Strategic level (that is data converted to information and assessed by analysts) and the movement of intelligence across the various consumers within the USG. Unmentioned, but essential to realize, is that the Department of Defense owns and operates very little of its own network infrastructure—it relies on commercial public and private operators for communications links around the globe. [JPG joint planning group](#)

[JWICS](#), though cryptographically separated from other traffic on these links, is still fundamentally reliant on commercial providers for the bulk of its bandwidth and availability.

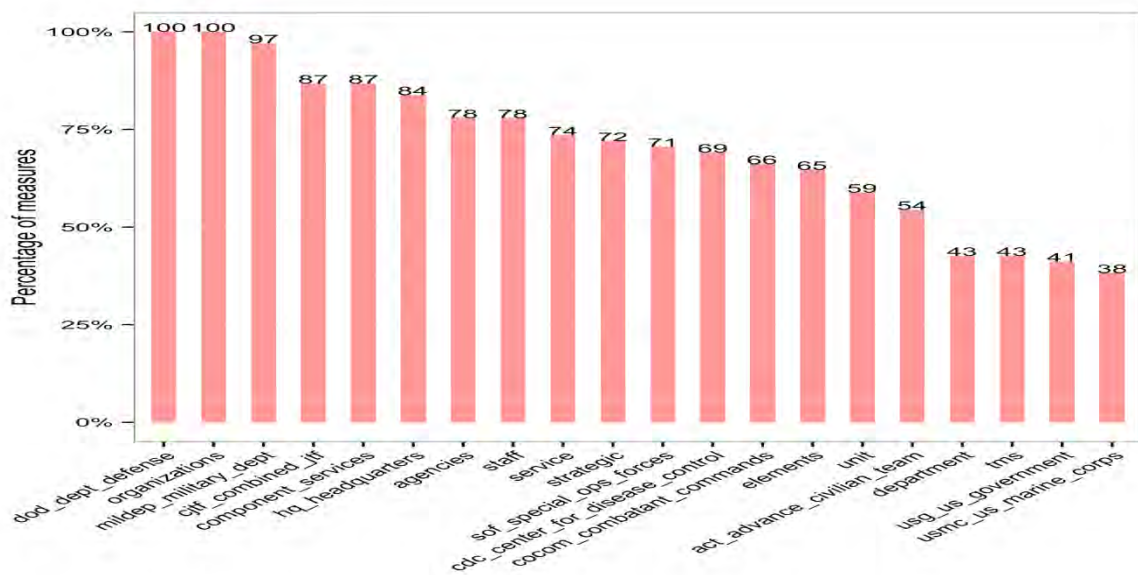


Figure 67: Recurring top ranked Organizations (top 20), strategic model

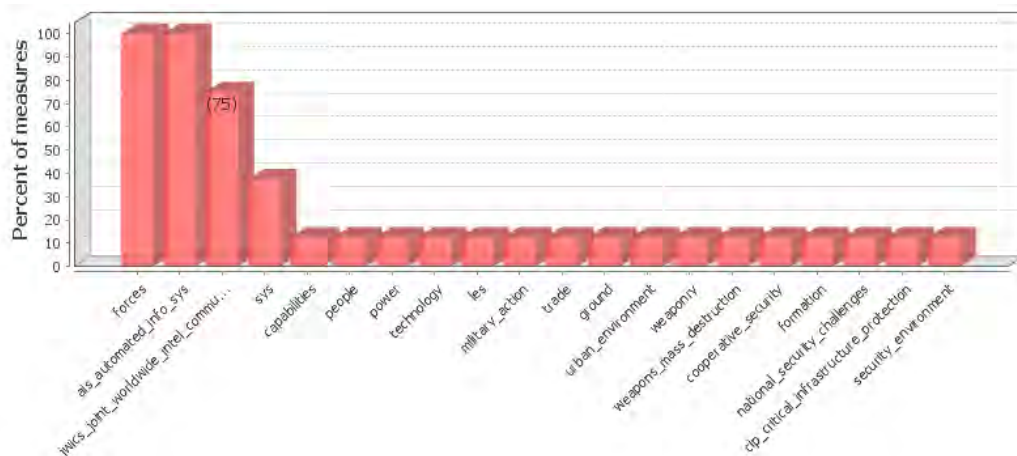


Figure 68: Recurring top ranked Recurring top ranked resources (top 3), strategic model

Expanding the window of analysis to the resources that appear in the top 20, [Figure 69](#), of these measures does not meaningfully clarify the importance of any particular IT resource. The top ranking forces and capabilities are generalized labels for resources available to the DoD, but not clearly useful for a resilience assessment. The over-all ranking of JWICS drops, while the importance of other resources enter the assessment window.

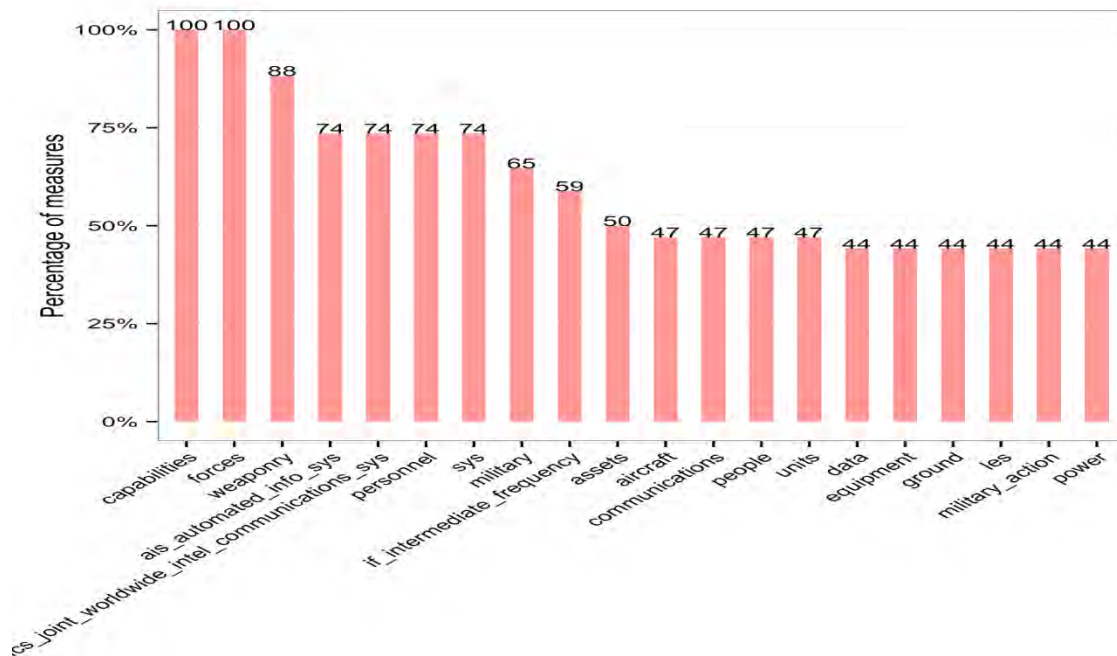


Figure 69: Recurring top ranked Recurring top ranked resources (top 20), strategic model

When disaggregating IT resources from non-IT resources, [Figure 70](#), the resource picture does not become more meaningfully clear. The items listed as appearing zero (0) percent of the time across the measures, are in alphabetical order from the ranks of entities in the same numerical category—meaning there are only six (6) entities that appear in the top three (3) of the resource-oriented measures. Like the merged resource view depicted above, these entities are too generalized for meaningful resilience assessment and planning.

The expanded view of the top twenty (20) finishers per measure does not yield any more clarity. This result, somewhat consistent across all three of these models, suggests that doctrine is potentially inadequate to perform rapid resource enumeration. It is more likely that organizations' documents about their standard operating procedures ([SOP](#)) within each of their war fighting functions would be a richer enumeration source.

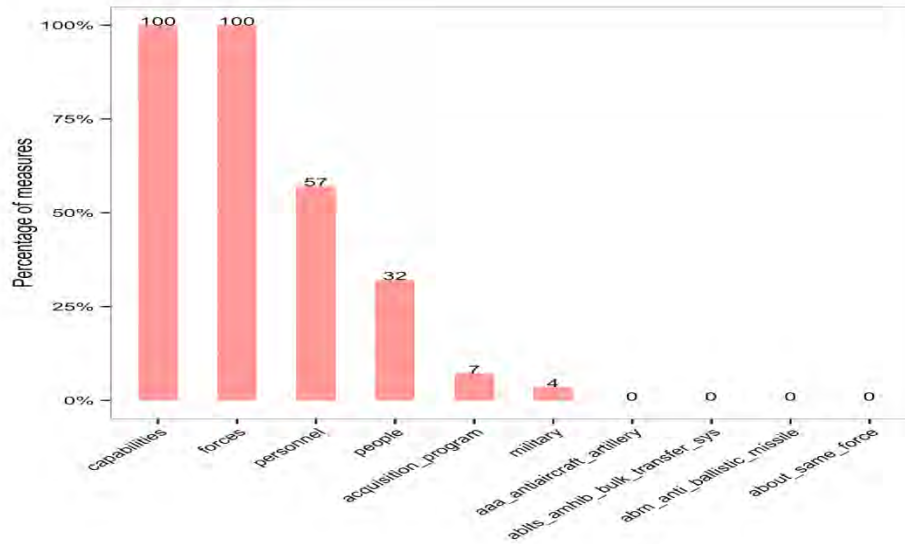


Figure 70: Recurring top ranked Non-IT resources (top 3), strategic model

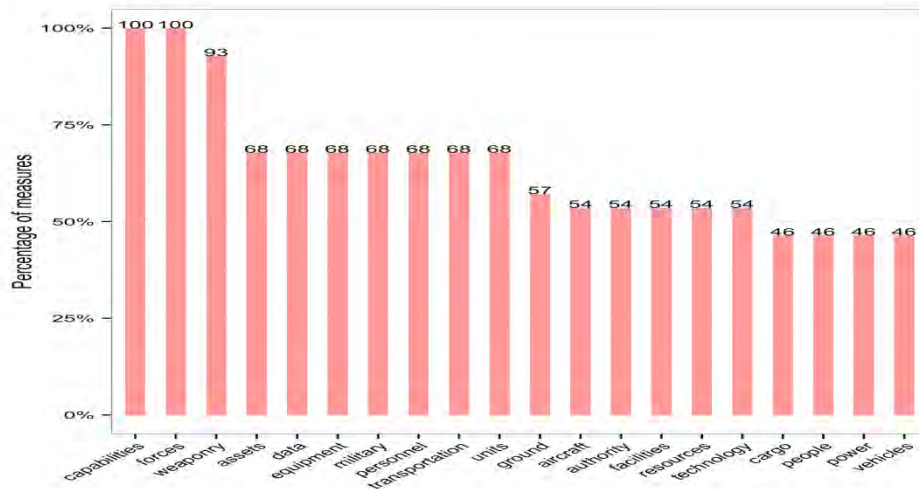


Figure 71: Recurring top ranked Non-IT resources (top 20), strategic model

The IT resources graphs, [Figure 72](#) and [Figure 73](#), reveal entities that are recognizable and reasonable to a Joint cyber familiar and aware member of DoD. The generic AIS is reflective of the pervasiveness of IT within the department. JWICS remains, as indicated in the aggregated view, consistently mentioned in the top twenty (20) finishers of each resource-centric measure. The top 20 graph indicates that there are a significant number of systems deemed by various authors as important, but there is wide variability in the authors' writings. The variability is potentially a good news review of available communications abilities. There is no single set of capabilities that form a critical IT hub that could disrupt the entire IT infrastructure of the DoD—at least not in doctrinal references.

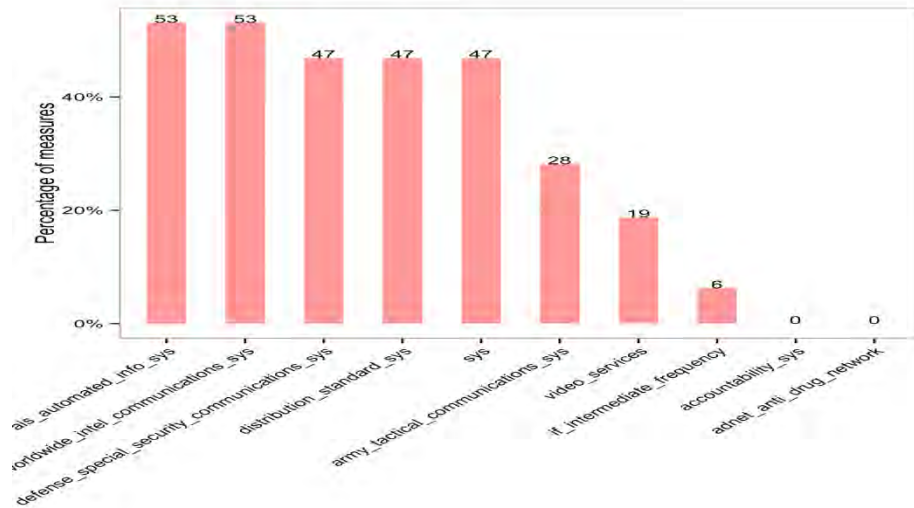


Figure 72: Recurring top ranked IT resources (top 3), strategic model

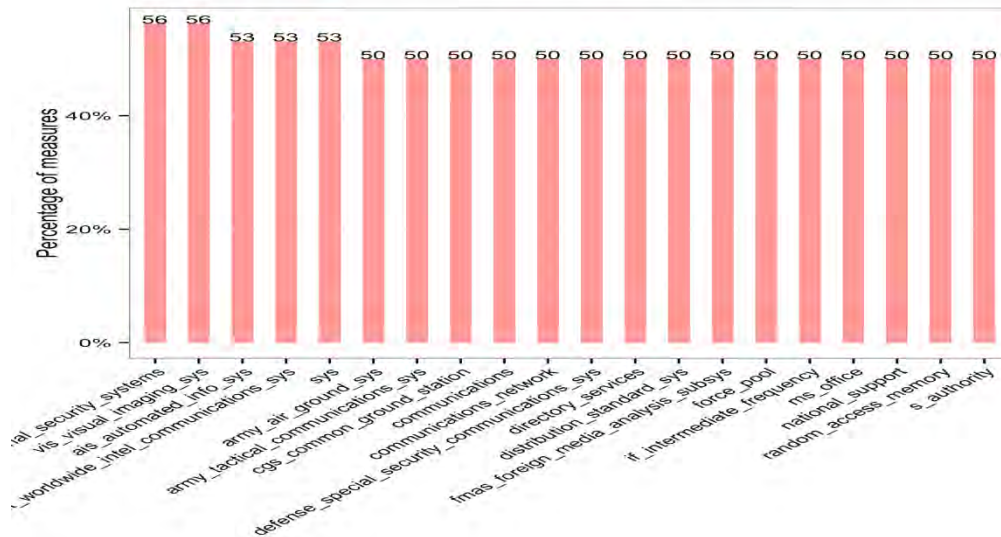


Figure 73 Recurring top ranked IT resources (top 20), strategic model

This section has demonstrated that the second of the three stopping conditions listed in [Table 18](#) is met for the Strategic model. The section later in this chapter entitled [Final Graphical Renderings - Strategic](#) provides the evidence of meeting the third stopping condition for the strategic model.

Final Graphical Renderings - Overview

Graph visualization is one of many ways to analyze the models in this dissertation, and is the third way (see also [Table 18](#)) to establish terminating conditions for the iterative D2M process. With 45+ networks per model, 18K+ nodes, and 1.4M+ nodes, visual representation of the entire metanetwork generally looks like a multi-colored ball of yarn—

sometimes visually striking but rarely fit to elucidate answers to questions. Instead, and as a demonstration of organizational face validity, I present in the following figures representations of the Organization x Organization networks for each of the two models.

A short discussion of what visual representations of networks and how ORA™ lets researchers make visualization choices follows. Each network represents the co-occurrence of each listed organization with other listed organizations. The numeric value for each link represents the number of times the co-occurrence happened within the relevant corpus. For example a link between a node labeled G_3 and G_2 indicates those two organizations co-occurred within a window of concepts in the relevant input corpus. A link weight of 20 for such a link, as an arbitrary example, would indicate there were 20 such co-occurrences in the relevant input corpus.

Table 24: Visualization options for organization x organization Models

Filter by link weights/values (per figure caption)
Recursively hide isolated nodes and pendant nodes (nodes with only one connection to another node).
Distance between nodes is a function of the link weight, with higher link weights representing stronger ties between nodes and hence visually closer together.
Nodes colored by a researcher imposed attribute defining approximate level of command within an Army tactical hierarchy, the Air Force operational hierarchy, and the strategic hierarchy. The colors are for high contrast and not for any doctrinal or semantic reflection of meaning, and are the first figure in each series of figures
Removal of nodes from graph whose level-of-warfare is ambiguous (left blank)

Final Graphical Renderings - Operational

The visualizations below are for the Operational model (Combatant Command to Numbered Air Force). I include four visualizations of the same model, at three levels of link-weight filtering and one filtered by the exogenously determined ‘level’ of command. Node colors per ‘level’ of command are shown in the legend in [Figure 74](#). [Figure 75](#) is the version with no filtering by link weight, and nodes with ambiguous levels of command colored in translucent green. This is a fairly typical ball of yarn for such a large network and is reflective of the challenges of rendering large numbers of meaningfully discrete objects. [Figure 76](#) however begins to reveal itself as closer to attaining face validity through its two principal colors, purple for the combatant command, blue for the Air Force Service Component ([USAFCENT](#)) and red and orange for various [AOC](#) elements. In this view, each of the five (5) principle divisions of the AOC are visible, as well as the cross functional teams and groups. In [Figure 77](#), the model reveals the even stronger links with the filtering

set to 15 or higher, though it is still clearly dominated by the purple joint and semi-joint elements of the Combatant Command, the Joint Air Force Component, and other elements associated with cyber operations. [Figure 78](#) depicts yet another level of filtering with links with edges 35 or higher depicted. Taken in isolation, a researcher might chose to interpret the filtered view of this weighted network as indicating that, from the 83 documents in the Operational corpus, the emphasis tends to be on the joint and mostly joint elements of this set of organizations.

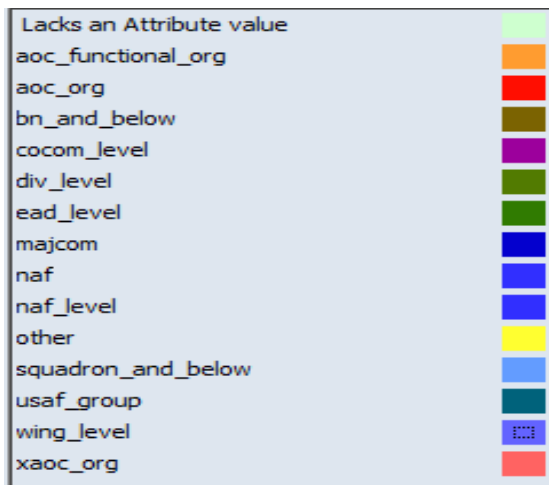


Figure 74: Node color legend for operational organization x organization visualizations

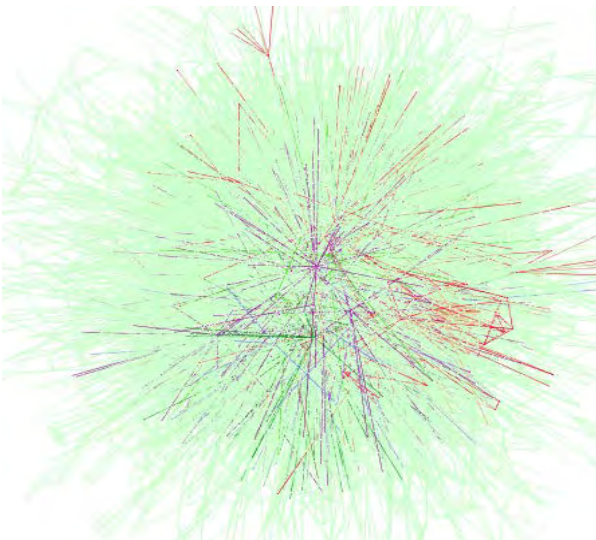


Figure 75: Operational org x org, no filtering by link weight

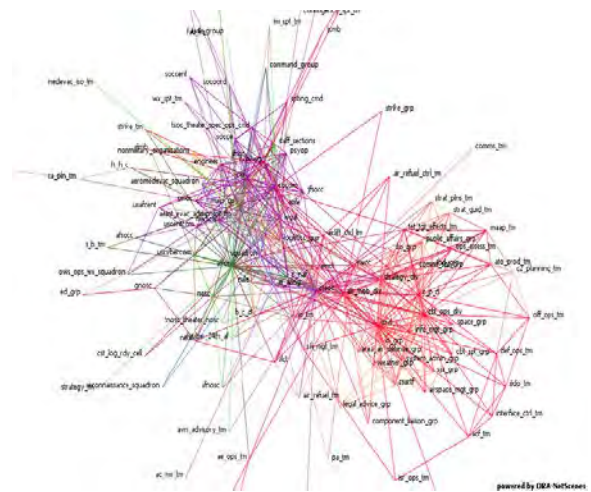


Figure 76: Operational org x org, filtering by level of warfare \neq blank (the level is unambiguously within scope, exogenously determined by researcher)

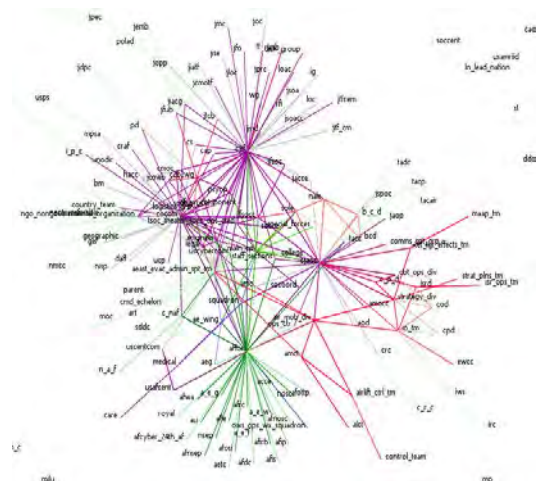
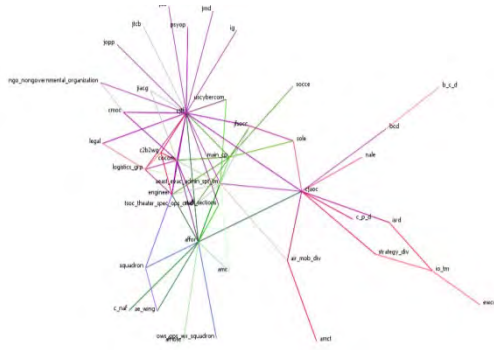
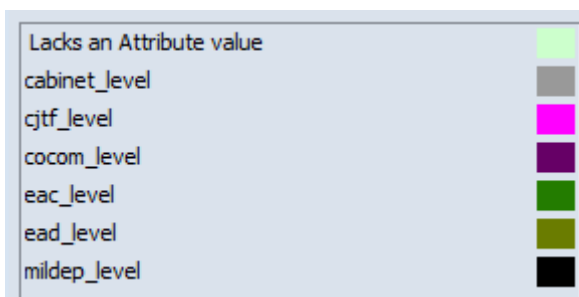


Figure 77: Operational org x org, filtering by link weight ≥ 15



Final Graphical Renderings - Strategic

The visualizations below are for the strategic model ([NCA](#) to [USSTRATCOM](#), [USCENTCOM](#), and [USCYBERCOM](#)). I include three versions of the same network, at three levels of link-weight filtering. [Figure 75](#), with no filtering at all, is reflective of the challenges of rendering large numbers of meaningfully discrete objects. Filtering the displayed links and nodes by link weight, it's apparent that a value of 15 ([Figure 76](#)) is insufficiently de-cluttered to make any reasonable [SME](#) assessment from visual inspection. By increasing the filter value to 35 (see [Figure 77](#)) it is becoming more apparent that each of the intended primary organizations are present, though it's indeterminate whether we have an excessive number of unnecessary organizations remaining in the model. The numerous exemplars for viewing the model reflect choices any researcher can make as part of their model-refinement process, and when to stop such refinements. Via visual inspection, a SME can confirm relevant organizations and suborganizations are present, prune nodes not in scope to the research question, and in the opposite sense, decide to not prune nodes based on unanticipated but present links between nodes. I also included DoD elements associated with how the Department, in accordance with the National Strategy for Cyber, has decided it will conduct cyber operations at the strategic level.



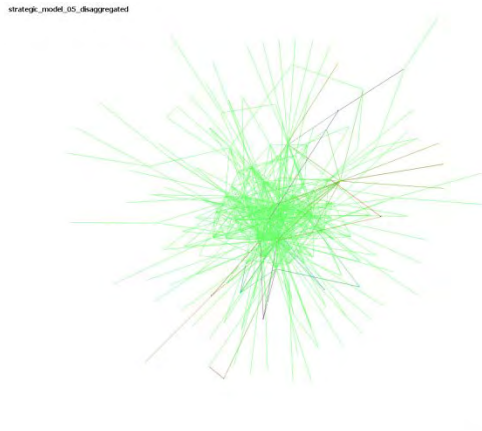


Figure 81: Strategic org x org, filtering by link weight ≥ 15

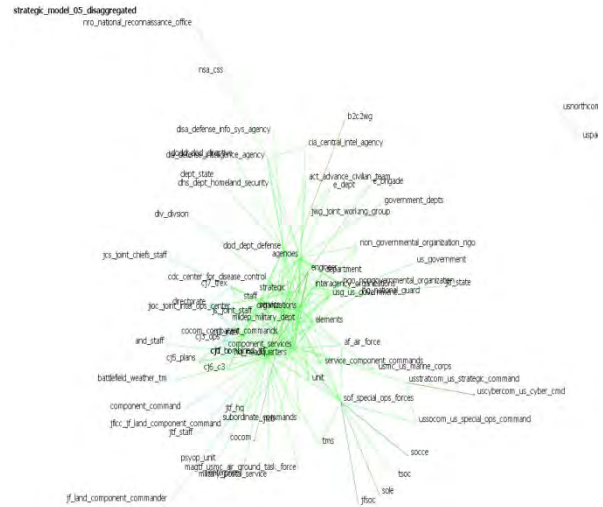


Figure 83: Strategic org x org, filtering by link weight ≥ 35

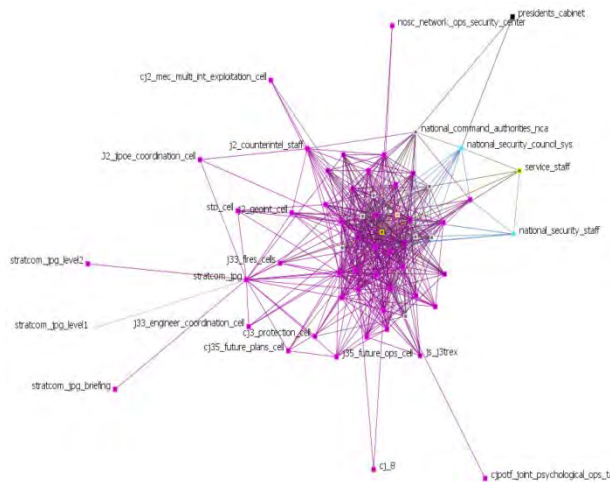


Figure 82: Strategic org x org, filtering by level of warfare \neq blank (the level is unambiguously within scope, exogenously determined by researcher)

Input Inconsistencies and Biases

Doctrine at the Joint and Services levels is frequently written by multiple authors over multiples months and years, with numerous editors, all of varying training and experience in the fields of technical and doctrine writing and editorial control. With that background and those limitations, it should surprise no one that there are inconsistencies between doctrine documents (e.g., assertions of primacy and need for adherence) as well as within doctrine documents (e.g., computer security as ‘commander’s business’ with implicit and sometimes explicit tones of ‘this is too complicated for commanders’).

I was aware of the possibility of biasing the input by over-selecting cyber security, information assurance, and other documents that would be focused on IT. To avoid this possibility, I deliberately avoided over selecting for such technology focused documents and focused on more general conduct of operations doctrine. I do not have evidence however that I hit the right mix, or that I over corrected and under selected for technology focused doctrine documents.

In the future work section I describe possible ways of quantifying the bias across documents, within documents, and identifying if those biases are effecting the resultant models. It may be infeasible to eliminate all forms of bias since the authors of the documents are unknown as are their own personal and professional tendencies.

Limitations of Text-Mining and D2M process

Text-mining as a method of constructing general organizations seems an imminently reasonable starting point for model construction. However there are difficulties and challenges associated with the use of free-form documents to derive a organizational meta-model.

The first and most obvious drawback is the use of pictures, charts, diagrams, and other visual explanatory material in the documents. The old saying that a picture is worth a thousand words requires pictures’ content be transcribed back into a text readable by the D2M process. A second significant drawback is where doctrine or other documents use tables and lists to convey semantic meaning via positioning or other stylistic mechanisms. The D2M process, as it exists now, does not capture the doer of an list of actions presented in a list form. The D2M process can read text in tables, but does not currently attempt to differentiate columns and their headings,

from rows and their headings. Semantic content then gets lost unless transcribed into a separate file.

The D2M process is also hampered in its ability to convey emphasis or valence. There can be proscriptive lists that the D2M process will completely miss the negative valence and intent. There can also be lists of items or actions that a particular agent or group of agents are responsible for, and the positive valence of the list gets lost, as well as the potential linking of the object noun(s) to every single sentence.

These shortcomings are, at present, overcome through model review and suggestions of SME input. The identification of valence, positive or negative sentiment in text is itself a field of research within the text-mining community, and I will defer to that community for advances in technology to reduce the workload of SMEs.

Summary of D2M process

This portion of the dissertation has discussed the origin of the data from which I have built two distinct models of portions of the US Department of Defense. Each model represents one simplified portion of the larger organization to assist demonstrating generalizability of the model building process. I have also presented a multi-step process as well as modifications of the CASOS [D2M process](#) to support the model construction in this acronym and jargon filled domain. Finally, I have presented the numerical descriptives of each of the models derived from this text-to-model process. Recall that though one deliverable of the dissertation is a process that can be followed by future researchers, and DoD modelers. Though it is a deliverable, the process is a means to an end. It is also a previously unavailable means that is significantly more rapid than any risk management framework compliance assessments in my professional experiences. This rapidity sets this process apart from other forms of organizational model construction. The process is also very accessible to un-augmented staff and supports the capturing and reflecting connections between and among nine (9) different node-types,

Changes to empirical models in support of Agent Based Modeling

I defer the discussion of the modifications to the empirical models to enable a near direct transition to the Construct simulation capability to the [Agent Based Models and Modeling](#) Chapter (on page [175](#)).

Conclusions

In the abstract and Introduction chapter, I listed four demands leaders should place on their organization to increase mission assurance in contested cyber environments. This chapter has addressed the second of those four demands: the ability to rapidly model their organization(s).

With this methodology, leaders and their subordinates can build graph models of their organizations with a small number of well defined steps. They can update their previous work to increase model validity or conduct excursions and forecasting. Organizations are no longer bound to the more traditional risk management framework snapshot in time assessment. There is no requirement to hire survey takers, expropriate time from the respondents, and adjust key-word coding per respondent. Instead, with the use of CASOS software tools, augmented by the DoD thesaurus and the work flow I've demonstrated and described, leaders can rapidly model their organization as their own documents describe it. Leaders can avoid the perception the model (or RMF assessment) is 'too old' to be accurate or relevant, helping them gain a more up to date level of confidence about their people, processes, and equipment. In this chapter, I introduced modified data to model processes, modified and built new computing capabilities and tools to support the automation-aided construction of multimode and multiplex organizational models from documents about the modeled organizations. This rapid modeling approach represents one of the principle contributions of the dissertation to the field of mission assurance and organizational resilience to contested cyber environments.

I have also postulated a meaningful research area into the statistical distributions of the metanetwork ontology—though I defer execution of that research to future work for myself or other researchers. On a last note, this chapter is the origin of the dissertation. With my professional history and outlook shaped by the US Army, I had originally approached this dissertation with the idea of helping the Army defeat the nation's enemies. It rapidly became apparent that applying this process to real world adversaries would require real world adversaries' documents, doctrine, and literature as well as appropriate translations. Securing access to such a dataset would be problematic at best. This difficulty had the natural outgrowth of demonstrating the process against friendly organizations. Presuming a competent enemy who seeks to understand us, they could do to us what I have demonstrated in this chapter—a automated method of supplementing the USAF CARVER method for targeting.

Network Analytics and Resilience

Numerous standard social network analysis ([SNA](#)) measures for single node types, single-mode measures, can offer indicators of general resilience—though they suffer from being unable to capture context outside the modeled types. Likewise, if organizations do not conduct assessments over time with sufficient frequency, their indicators and assessments may fail to capture enough information for meaningful conclusions—or worse, woefully misinformed conclusions. It is entirely feasible that depending on the timing of pre- and post event data gathering (see also [Figure 85](#)), assessments would completely miss any indicators of performance-degrading events. Such ignorance in the presence of data is one of numerous justifications for dynamic network analysis ([DNA](#))—that is the longitudinal application of SNA measures to a data set or organization. Longitudinal study of organizations and the events that affect those organizations can be resource intensive above and beyond the investment in time. Organizations must be able to identify their sense of ‘normal,’ identify when contested cyber environments begin and end, and identify the affect people, systems, processes, and other structural elements. Organizations must also be able to quantify those effects with a trustworthy methodology and meaningful effects.

To the requirements above, this chapter offers an exposition of theory applied to the domain of resilience to contested cyber environments. Exposition is through application of quantitative SNA techniques to the models created in the Data-to-Model ([D2M](#)) process of the preceding chapter. The application of quantitative analytic techniques to the models addresses the first of the four demands I specified in the abstract: leaders should require assessments be more than analogical, anecdotal or simplistic snapshots in time. I extened the fields of SNA and organizational behavior by providing a static measure of resilience as a function of near-isolation of agents, tasks, resources, and knowledge.

Harkening back to the dissertation work flow of [Figure 35](#) and zooming in between the creation of the models and the augmentation leading to simulation, [Figure 84](#) is another breadcrumb to assist the reader in knowing where this chapter fits in the workflow of the dissertation.

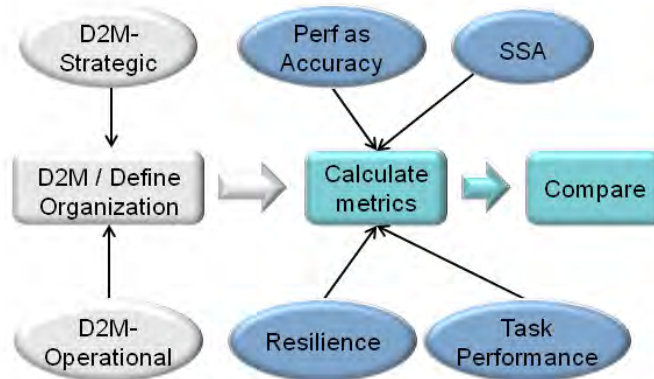


Figure 84: Dissertation workflow static analysis prior to augmentation for agent based modeling

Resilience in what context?

Like (Pflanz, 2012; Pflanz & Levis, 2012) and revisiting [Figure 2, now shown as Figure 85](#), a graph depicting the dynamic nature of resilience is useful to convey a more complete understanding.

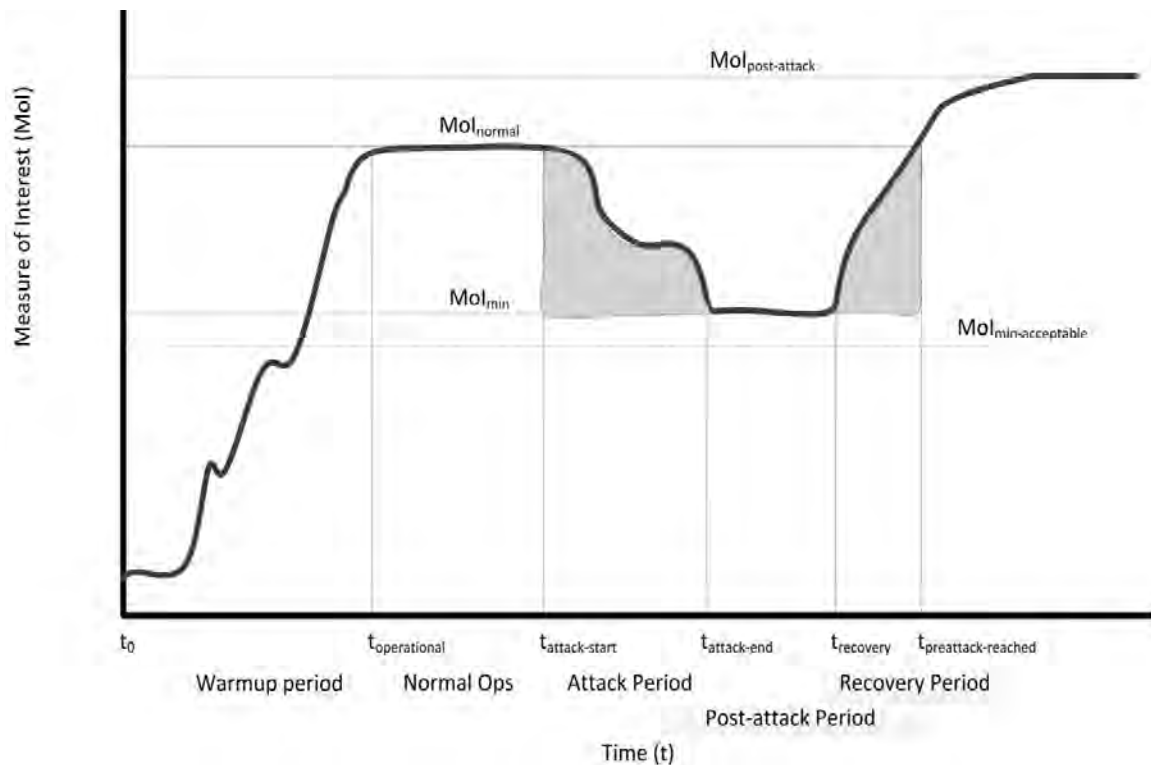


Figure 85: Dynamic visualization of resilience for an arbitrary measure of interest (MoI)¹²

In this Figure, there is a span of time from t_0 to t_{warmup} that reflects the possible values of a Measure of Interest ([MoI](#)) prior to reaching a pre-contested-environment equilibrium. As noted

¹² (Morgan & Lanham, 2012)

by Pimm (1984), without equilibrium, resilience is indefinable. During the time of normal operations ($\text{MoI}_{\text{normal}}$), the organization achieves some level of equilibrium with variance within some acceptable tolerances. The figure also depicts the beginning of an attack ($t_{\text{attack-start}}$), or some other cause for a negative Confidentiality-Integrity-Availability (CIA) effect(s). While the attack is ongoing, the attack should be having some effect on the MoI, though it may not be consistent, statistically or operationally significant—absent an effect, there is no rational reason to expend resources to deal with the attack. As shown, there is an approximate stair step halfway through the attack...as just one of an infinite variety of possible impacts on the MoI (e.g. instantaneous drop, linear or step-wise linear drop, logarithmic drop, quadratic drop). At some point-in-time, the attack ends ($t_{\text{attack-end}}$), though there is no guarantee that the organization or its agents are aware of the specific end time—nor for that matter are they assured of being aware of a specific start time ($t_{\text{attack-start}}$). The chart above depicts a quiescent period after the attack and before ‘recovery’ begins (t_{recovery}), or before the MoI rises above the minimum performance reached as a consequence of the attack.

There is no requirement for recovery to start immediately, as the attack may have effects on the MoI that outlast the attack itself. It’s also important to note that there is a space between the minimum performance ($\text{MoI}_{\text{min-acceptable}}$) for this MoI and a minimally acceptable threshold set, *a priori*, by one or more leaders of an organization of interest. This threshold may have been set, or may simply be a generalized statement by leadership akin to ‘no performance drop is acceptable!’ This picture does not depict a return to pre-attack levels for this MoI (at $t_{\text{pre-attack reached}}$), indeed there is no universal requirement in definitions of resilience that such a return to pre-event levels occur, notwithstanding Bishop (2011). To be sure, in the happy situation shown above, the forecast is that the attack/attacker makes the organization better in this MoI than they might otherwise have become, with adaptation as a likely explanation.

In an attack, however, where the MoI_{min} drops below $\text{MoI}_{\text{min-acceptable}}$, the MoI for the modeled organization would have low resilience, and potentially low-survivability. Such a situation would make recovery all the more daunting as first recovery efforts would be geared to re-gaining the $\text{MoI}_{\text{min-acceptable}}$ level of performance.

Static resilience indicators

Deciding which SNA-measures an organization can or should use to indicate resilience to cyber events is a fundamental task for any meaningful program of assessment and improvement. The decision may be existing-data driven—a measure with no supporting data is a theoretical achievement un-anchored to any organizational reality. Of course, lack of data during the decision process can itself drive efforts to establish a recurring data collection mechanism that, ideally, imposes little differential loading on the organization itself. A brief example of SNA-measures and their applicability to the domain of cyber resilience follows.

When a resilience question relates to information or belief diffusion, a researcher could use changes in measured pre- and post event “communication speed” (Kathleen M. Carley, Pfeffer, Reminga, Storrick, & Columbus, 2012)—where the longest path length of the Agent-by-Agent ($\mathbb{A}\mathbb{A}$) network is an indicator of the speed that any arbitrary message can pass across the modeled network. This communication speed model is inappropriate to modeling specific technical-channel flows—for that goal a tool such as OMNet++ may be more applicable. However, realizing that humans frequently have more than one method of communicating with other humans, this measure abstracts away the details of channel selection, capacity, utilization, and congestion. In this abstracted manner, this model provides an indicator of possible changes to message passing speeds pre- and post event, and allows a quantitative assessment of the impact(s) to such message passing.

Negative changes in an organization’s Resource-by-Resource ($\mathbb{R}\mathbb{R}$) network (e.g., loss of links or nodes in the $\mathbb{R}\mathbb{R}$ matrix), indicating possible loss of system-to-system communications links or unfulfilled inter-dependencies are another application of SNA to the myriad facets of resilience assessment and engineering. Not all changes are necessarily negative in their impacts. It is entirely feasible that the loss of access to one or more systems by one or more agents and their organizations may lead the organization to successful adaptive behavior. Where the behavior is deleterious to the desired organizational outcomes, leadership and assessors have succeeded in identifying mal-adaptive behavior as well. Before discussing further applications of SNA measures to cyber resilience assessments, it is appropriate to look at the results of measures calculations on the three models in the dissertation: tactical level; operational level; and strategic level.

This application of network analytics to organizational resilience is akin to the [CARVER](#) method of targeting used by the US military and some of its military allies. US Joint and Service doctrine discuss [CARVER](#) (Criticality, Accessibility, Recuperability, Vulnerability, Effect and Recognizability) as a methodology to help quantify the inputs to the targeting decision processes—what resources, organizations, or people should the military apply force against, to what effect, and for how long should the effect last. With CARVER as a near analog, it's an easy leap to using standard centrality measures (e.g., inDegree, outDegree, geodesic centrality (Freeman, 1977)) for agents and message-passing resources. These measures have other analogs in the idea of span-of-control (the number of direct-report subordinates a leader can effectively manage).

Metanetwork resilience indicators

Several metanetwork-based measures are also suggestive of potentially useful measures of interest. A partial list, primarily those contributing to the new measure 'resilience' is in [Table 25](#), with a more complete list in [Table 26](#).

Network measures, in particular the general network/organization measures shown below, would be infeasible without multimode networks. Calculations using matrix algebra support the creation of measures such congruence between knowledge and resources available and that needed for task completion. The same is true for the multimode assessment of cognitive demand (expanding past the effort humans expend to keep their social networks to the effort humans expend to maintain their social networks, manage their resources, and execute their tasks). Finally, Graham's work on shared situation awareness ([SSA](#)) would be infeasible without the added information in a metanetwork representation of an organization.

ORA™, with over 170 measures, helps assess static resilience in the two models using immediate impact assessments or the following metrics applied to the metanetwork using entropic and targeted node removal. A sampling of those measures are below in [Table 25](#).

Table 25: A sample of metanetwork measures for indicators of resilience

Measure	Meaning from Carley (2002d) and ORA™ Help
Performance as Accuracy	How accurately agents can perform their assigned tasks based on their access to knowledge and resources.
Communication Congruence	Measures to what extent the agents communicate when and only when it is needful to complete tasks. Perfect congruence requires a symmetric Agent x Agent

	network.
Knowledge Congruence	Across all agents, the knowledge that agents lack to do their assigned tasks expressed as a percentage of the total knowledge needed by all agents.
Key Node Identification	Using Key Entity reports
Shared Situation Awareness (SSA)	A function of Eigen vector centrality, social demographic similarity, and physical proximity. High values correspond to having a better understanding of what others are doing.
Resilience (new)	A function of near isolated status of knowledge, resources, and tasks, as well as organizational needs and wants with respect to knowledge and resources. High Values indicate high resilience to contested cyber environments.

New and adjusted metanetwork resilience indicators

There are two sets of new measures of resilience under consideration. The first is a single measure that combines several existing measures. The second is a set of measures that provide over time assessment, and therefore requires over time data—in this dissertation generated through simulation and discussed in the next two chapters.

The first point-in-time measure is a multivariable function shown in (14). This is a multivariable function of normalized network access indices for knowledge, resources and tasks, organizational needs and the organizational waste. Access indices are reflections of near isolation, organizational needs reflects shortfalls in knowledge and resources needed to do tasks, and organizational waste represents knowledge supplied to tasks (via agents) that tasks do not need for their execution. The final three-part result is in (14), with the incremental steps to build to the equation shown in (15) through (35) along with additional definitions and explication for each component. Exogenous weighting factors, α , β , and λ are shown as well, though for this dissertation I set them to one (1) in the absent of evidence supporting other values. I have drawn and derived this measure from (Kathleen M. Carley & Pfeffer, 2012c; Kathleen M. Carley, Juergen Pfeffer, et al., 2012) with minor axial shifts.

$$Resilience = \alpha \left(\frac{1}{1 + e^{\mathbb{K}'_a}} + \frac{1}{1 + e^{\mathbb{R}'_a}} + \frac{1}{1 + e^{\mathbb{T}'_a}} \right) + \beta \left(\frac{1}{1 + e^{n_{knowledge}}} + \frac{1}{1 + e^{n_{resources}}} \right) + \lambda \left(\frac{1}{1 + e^{-w_{knowledge}}} + \frac{1}{1 + e^{-w_{resources}}} \right) \quad (14)$$

Equation 14: Structural resilience as a new metanetwork calculation

The three-part access index component, multiplied by α , is a measure of near isolation for three node types: knowledge, tasks, and resources. Near isolation is another way of referring to a single point of failure. (SPOF) —albeit possibly irrelevant to specific questions of interest. For the agent node set, (15) shows how to compute the knowledge access index. In English, for each agent, a possibly empty set of knowledge entities (\mathbb{K}) exists of knowledge to which only the one agent has access. Additionally, the agent (ego) with access connects to only one other agent (alter)—the ego is a pendant with respect to all alters.

$$\forall \mathbb{A}, \mathbb{K}_a = \left\{ k \mid \mathbb{A}\mathbb{K}(i, k) \wedge \left(\sum \mathbb{A}\mathbb{K}(: k) = 1 \right) \wedge \left(\sum \mathbb{A}\mathbb{A}(i :) = 1 \right) \right\} \quad (15)$$

Equation 15: Access index as reflection of criticality through near isolation (Kathleen M. Carley, Juergen Pfeffer, et al., 2012)

The intuition is that the effect of this type of SPOF corresponds to an inverse sigmoid function (aka S-curve), such that low numbers of SPOFs correspond to high levels of structural resilience. I normalize the access index by the magnitude of its source node set. I then segment the result into 12 bins—12 bins allows the output curve to align with the Army’s (though not Air Force or Joint) color coding scheme for unit combat effectiveness¹³. With normalized results of (15) ranging from [0, 1], the sigmoid function must shift to the right to reflect zero near isolates equate to the maximal output of the function ($x=0 \rightarrow f(x)=1$). The exponent of the sigmoid function is shown in (16) with the final sigmoid function shown in (17).

$$\mathbb{K}'_a = \frac{\sum \mathbb{K}_a}{|\mathbb{K}| / 12} - 6 = \frac{12 \times \sum \mathbb{K}_a}{|\mathbb{K}|} - 6 \quad (16)$$

Equation 16: Normalized summation of a model’s knowledge access index, agents aggregated

¹³ The four (4)-color ‘Gumball’ method of representing unit effectiveness at a glance is green, amber, red, black. These colors corresponds to combat capable/100%-85% strength, combat capable/70-84% strength, Combat Ineffective/50-69% strength, and requires reconstitution/<50% strength (Headquarters Department of the Army, 2010). In this color-coding scheme, a decrease in a measure of 30-50% corresponds with an organization in need of reconstitution/regeneration before receiving additional missions. Decreases of 15% or less correspond with no change in visual representation of the measure—the color code remains ‘green.’

$$Knowledge_{AccessComponent} = \frac{1}{1 + e^{\mathbb{K}'_a}} \quad (17)$$

Equation 17: Knowledge access component sigmoid, right shifted six values, in 12 bins

Equation (17) depicts all types of agents aggregated into a single group. In this dissertation I disaggregated Agents (nominally humans or roles humans fill) and IT Agents (nominally computer-based systems or capabilities that process, store, manipulate transmit and receive data). To accommodate this disaggregation I modified (16) by summing the two ORA™-calculated Knowledge Access Indices before normalizing. This modification is shown in (18) with the consequent update to (17) reflected in (19).

$$\mathbb{K}'_{a+ita} = \frac{12 \times (\sum \mathbb{K}_a + \sum \mathbb{K}_{ita})}{|\mathbb{K}|} - 6 \quad (18)$$

Equation 18: Normalized summation of a model's knowledge access index, agents disaggregated

$$Knowledge_{AccessComponent} = \frac{1}{1 + e^{\mathbb{K}'_{a+ita}}} \quad (19)$$

Equation 19: Knowledge access component sigmoid, right shifted six values, in 12 bins, agents disaggregated

Identical calculations then occur for tasks as shown in (20). Calculations for Resource Access Index had to accommodate the combinatoric effects of disaggregating IT resources from Resources as well as disaggregating Agents and IT Agents and is shown in (21).

$$\mathbb{T}'_{a+ita} = \frac{12 \times (\sum \mathbb{T}_a + \sum \mathbb{T}_{ita})}{2 \times |\mathbb{T}|} - 6 \quad (20)$$

Equation 20: Normalized summation of a model's task access index, agents disaggregated¹⁴

$$\mathbb{R}'_{ra+rita+itra+itrita} = \frac{12 \times (\sum \mathbb{R}_a + \sum \mathbb{R}_{ita} + \sum \mathbb{ITR}_a + \sum \mathbb{ITR}_{ita})}{2 \times |\mathbb{R} + \mathbb{ITR}|} - 6 \quad (21)$$

Equation 21: Normalized summation of a model's resource and IT resource access index, agents disaggregated

The use of (19), (20), and (21) to build the combined access index component causes that component to look like (22) below.

$$Access\ Index\ Component = \alpha \left(\frac{1}{1 + e^{\mathbb{K}'_{a+ita}}} + \frac{1}{1 + e^{\mathbb{R}'_{ra+rita+itra+itrita}}} + \frac{1}{1 + e^{\mathbb{T}'_{a+ita}}} \right) \quad (22)$$

Equation 22: Access Index Component, adjusted for disaggregation of Agent and Resource node sets

¹⁴ ORA™ does not yet support direct calculation of task access index. To accomplish this, I recoded the 'Task' node set as a 'Knowledge' node set and re-executed the knowledge access index calculation report in ORA™.

A 2D projection of the sum of two of the above indices is below, with the addition of the third index left as an exercise for the reader. It is easy to discern that when there are no SPOFs, the highest score shown for two (2) indices is two (2). The Access Index Component is therefore a function with a range of $[0, 3]$ with three (3) being the best possible score, representing no SPOFs for tasks, knowledge, or resources.

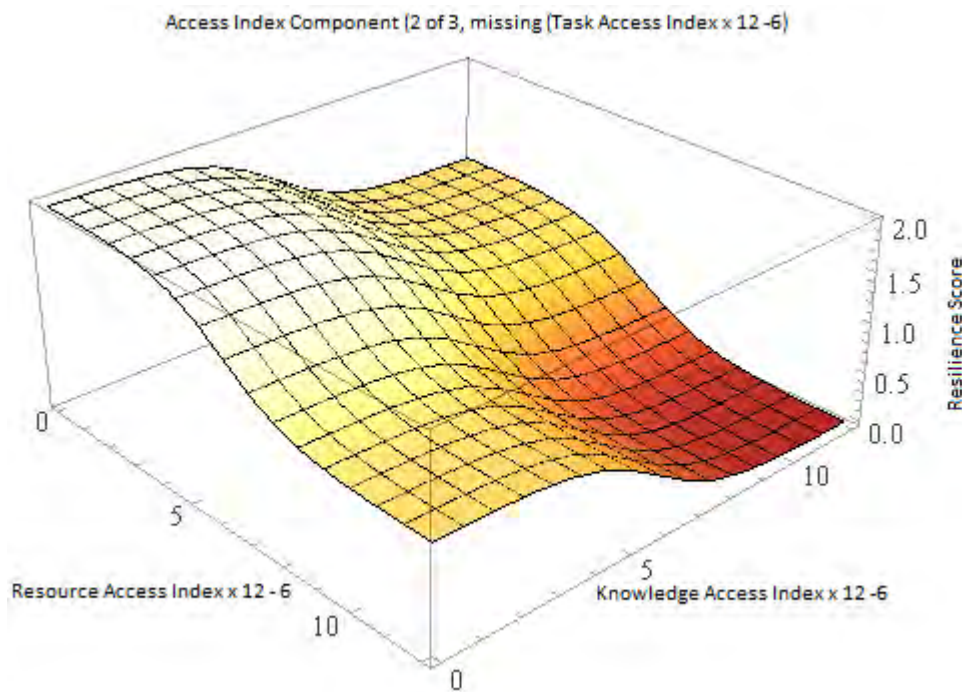


Figure 86: 2D projection of 3D rendering of two access indices

The next portion of building (14) is the calculation, at an organization level, of the knowledge and resource shortfalls. Within ORA™, the measures names are *congruenceOrgTaskKnowledgeNeeds* and *congruenceOrgTaskResourceNeeds*. *congruenceOrgTaskKnowledgeNeeds* reveals “Across all tasks, the knowledge that tasks lack expressed as a percentage of the total knowledge needed by all tasks” (Kathleen M. Carley, Juergen Pfeffer, et al., 2012). A value of zero (0) is an excellent result for both measures. Using the same number of bins as the access index calculations, I again right shift the curve six (6) values. I also translate the percentage to one of 12 bins as shown in (25) and then used as input into a standard sigmoid function show in Figure 87. Figure 87 is a reduced form of the Access Index Component with only two (2) functions summed, causing a reduction in the range from $[0,3]$ to $[0, 2]$. Zero (0) is indicative there are no tasks lacking knowledge of any variety.

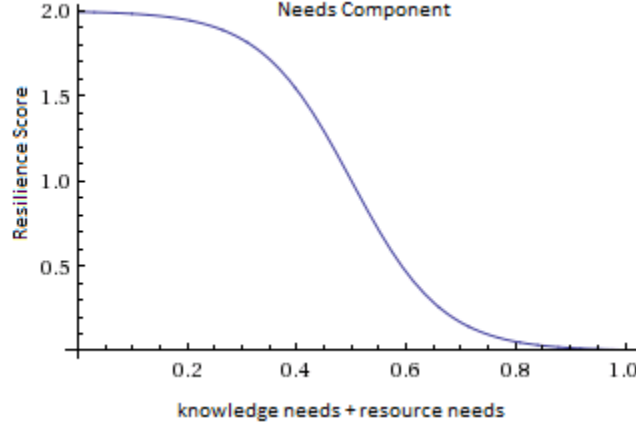


Figure 87: Sigmoid function of knowledge + resource needs component, low input values best

$$\mathbb{S}_k = \mathbb{A}\mathbb{T}' \times \mathbb{A}\mathbb{K} \quad (23)$$

Equation 23: Tasks with needed knowledge via assigned agents (Kathleen M. Carley, Juergen Pfeffer, et al., 2012)

$$n_{knowledge} = \frac{\sum_{t=1}^{|\mathbb{T}|} \sum_{k=1}^{|\mathbb{K}|} \mathbb{K}\mathbb{T}'(t,k) \times (\mathbb{S}_k(t,k) = 0)}{\sum \mathbb{K}\mathbb{T}} \quad (24)$$

Equation 24: Percentage of knowledge not provided by agents assigned to tasks (Knowledge Needs) (Kathleen M. Carley, Juergen Pfeffer, et al., 2012)

$$n'_{knowledge} = (n_{knowledge} \times 12) - 6 \quad (25)$$

Equation 25: Knowledge needs, right shifted 6 values, in 12 bins

$$Needs_{KnowledgeResource} = \frac{1}{1 + e^{n'_{knowledge}}} + \frac{1}{1 + e^{n'_{resource}}} \quad (26)$$

Equation 26: Needs Component as sum of two sigmoid needs functions, right shifted 6 values, in 12 bins

Again, there are modifications to (26) necessary due to the disaggregation of agents and IT agents. To merge and normalize the $n_{knowledge}$ value for agents and IT agents, it is necessary to unwind the percentage values of each, and recalculate a normalized value. This process is in (27).

$$n'_{knowledge_{agent+itagent}} = 12 \times \frac{(n_{knowledge_{agent}} \times |\mathbb{T}|) + (n_{knowledge_{itagent}} \times |\mathbb{T}|)}{2 \times |\mathbb{T}|} - 6 \quad (27)$$

Equation 27: *congruenceOrgTaskKnowledgeNeeds* with disaggregated agents and IT agents (Kathleen M. Carley, Juergen Pfeffer, et al., 2012)

$$\mathbb{S}_r = \mathbb{A}\mathbb{T}' \times \mathbb{A}\mathbb{R} \quad (28)$$

Equation 28: Tasks with needed resources via assigned agents (Kathleen M. Carley, Juergen Pfeffer, et al., 2012)

$$n_{resource} = \frac{\sum_{t=1}^{|T|} \sum_{r=1}^{|R|} \mathbb{RT}'(t,r) \times (\mathbb{S}_r(t,r) = 0)}{\sum \mathbb{RT}} \quad (29)$$

Equation 29: Percentage of resources not provided by agents assigned to tasks (Kathleen M. Carley, Juergen Pfeffer, et al., 2012)

$$n'_{resource} = (n_{resource} \times 12) - 6 \quad (30)$$

Equation 30: Resource needs, right shifted 6 values, in 12 bins

The modifications to [\(30\)](#) due to the disaggregation of resources and IT resources follows the same pattern as the modification for $n_{knowledge}$. With two disaggregations, IT Agents and IT resource, there are four percentage values to unwind and renormalize This process is shown in [\(31\)](#).

$$n'_{resource} = 12 \times \frac{(n_{resource_{agent}} \times |\mathbb{R}|) + (n_{resource_{inagent}} \times |\mathbb{R}|) + (n_{itresource_{agent}} \times |\mathbb{ITR}|) + (n_{itresource_{inagent}} \times |\mathbb{ITR}|)}{2 \times |\mathbb{R} + \mathbb{ITR}|} - 6 \quad (31)$$

Equation 31: *congruenceOrgTaskResourceNeeds* with disaggregated agents and IT agents (Kathleen M. Carley, Juergen Pfeffer, et al., 2012)

The measure *congruenceOrgTaskKnowledgeWaste* reveals “Across all tasks, the knowledge that agents have that are not required to do their assigned” (Kathleen M. Carley, Juergen Pfeffer, et al., 2012). Intuitively, having extra knowledge within an organization is inefficient but potentially useful in some crisis or exigency. As such, this aspect of the resilience score uses an inverted sigmoid function, indicating that zero (0) waste is bad, and that superfluous knowledge or resources are good. Using the same number of bins as the access index calculations, I again right shift the curve six (6) values as well as translate the percentage to one of 12 bins as shown in [\(36\)](#) and used as input into [Figure 88](#).

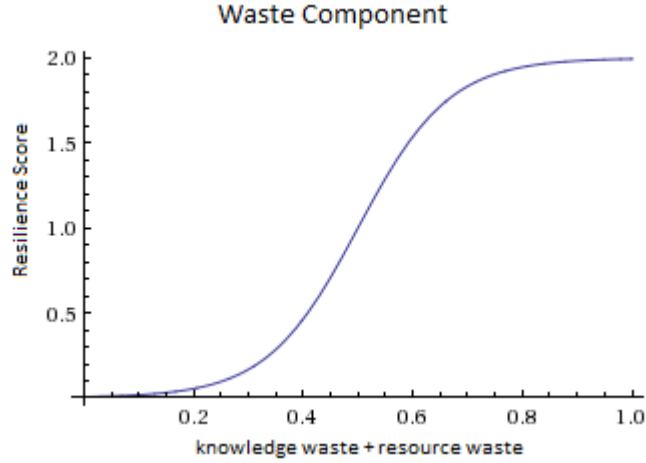


Figure 88: Sigmoid function of Knowledge + Resource Waste Component, high input values best

$$w_{knowledge} = \frac{\sum_{k=1}^{|\mathbb{K}|} S_k(t, k) \times \overline{\mathbb{K}\mathbb{T}'}(t, k)}{\sum_{k=1}^{|\mathbb{K}|} S_k(t, k)} \quad (32)$$

Equation 32: Percentage of knowledge not used for tasks assigned to agents (Kathleen M. Carley, Juergen Pfeffer, et al., 2012)

$$w'_{knowledge} = (w_{knowledge} \times 12) + 6 \quad (33)$$

Equation 33 Knowledge waste, right shifted 6 values, in 12 bins

Again, there are necessary modifications to (33) due to the disaggregation of agents and IT agents. To merge and normalize the $w_{knowledge}$ value for agents and IT agents, it is necessary to unwind the percentage values of each, and recalculate a normalized value. This process is shown in (34).

$$w'_{knowledge} = 12 \times \frac{(w_{knowledge_{agent}} \times |\mathbb{T}|) + (w_{knowledge_{itagent}} \times |\mathbb{T}|)}{2 \times |\mathbb{T}|} + 6 \quad (34)$$

Equation 34: *congruenceOrgTaskKnowledgeWaste* with disaggregated agents and IT agents (Kathleen M. Carley, Juergen Pfeffer, et al., 2012)

$$w_{resource} = \frac{\sum_{r=1}^{|\mathbb{R}|} S_r(t, r) \times \overline{\mathbb{R}\mathbb{T}'}(t, r)}{\sum_{r=1}^{|\mathbb{R}|} S_r(t, r)} \quad (35)$$

Equation 35: Percentage of resources not used for tasks assigned to agents (Kathleen M. Carley, Juergen Pfeffer, et al., 2012)

$$w'_{resource} = (w_{resource} \times 12) + 6 \quad (36)$$

Equation 36: Resource ‘Waste,’ right shifted 6 values, in 12 bins

The modifications to (36) due to the disaggregation of resources and IT resources follow the same pattern as the modification for $w_{knowledge}$. With two disaggregations, IT Agents and IT resource, there are four (4) percentage values to unwind and renormalize This process is shown in (37).

$$w'_{resource} = \frac{6 + 12 \times \left(w_{resource_{agent}} \times |\mathbb{R}| + (w_{resource_{itagent}} \times |\mathbb{R}|) + (w_{itresource_{agent}} \times |\mathbb{ITR}|) + (w_{itresource_{itagent}} \times |\mathbb{ITR}|) \right)}{2 \times (|\mathbb{R}| + |\mathbb{ITR}|)} \quad (37)$$

Equation 37: *congruenceOrgTaskResourceNeeds* with disaggregated agents and IT agents (Kathleen M. Carley, Juergen Pfeffer, et al., 2012)

$$Waste_{KnowledgeResource} = \frac{1}{1 + e^{-w'_{knowledge}}} + \frac{1}{1 + e^{-w'_{resource}}} \quad (38)$$

Equation 38: Waste Component as sum of two sigmoid waste functions, right shifted 6 values, in 12 bins

A 2D projection of (14) is shown in Figure 89 as well as a surface mapping of the interaction between a single growth curve (i.e. a single waste value) and a single decay curve (e.g., a single access index value or a single needs value) in Figure 90. A more comprehensive (for output values) surface depiction is in Figure 91. All three of these figures depict that the ideal resilient organization should have no near isolates, maximal excess knowledge and resources (e.g., twice what is minimally necessary), and no needs. They also show that the least resilient organization is hyper-efficient in knowledge and resource distribution with no waste whatsoever. The least resilient organization also has the degenerate case that all tasks, resources, and knowledge are near isolates and accessible only through agents that are pendants. Finally the least resilient organization has every task short of necessary knowledge and resources.

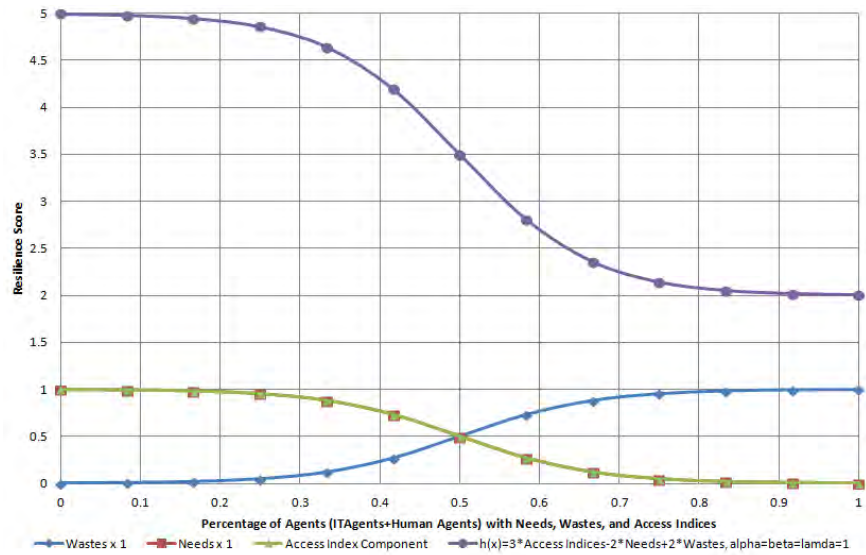


Figure 89: 2D rendering of resilience score, as function of access indices, wastes, and needs

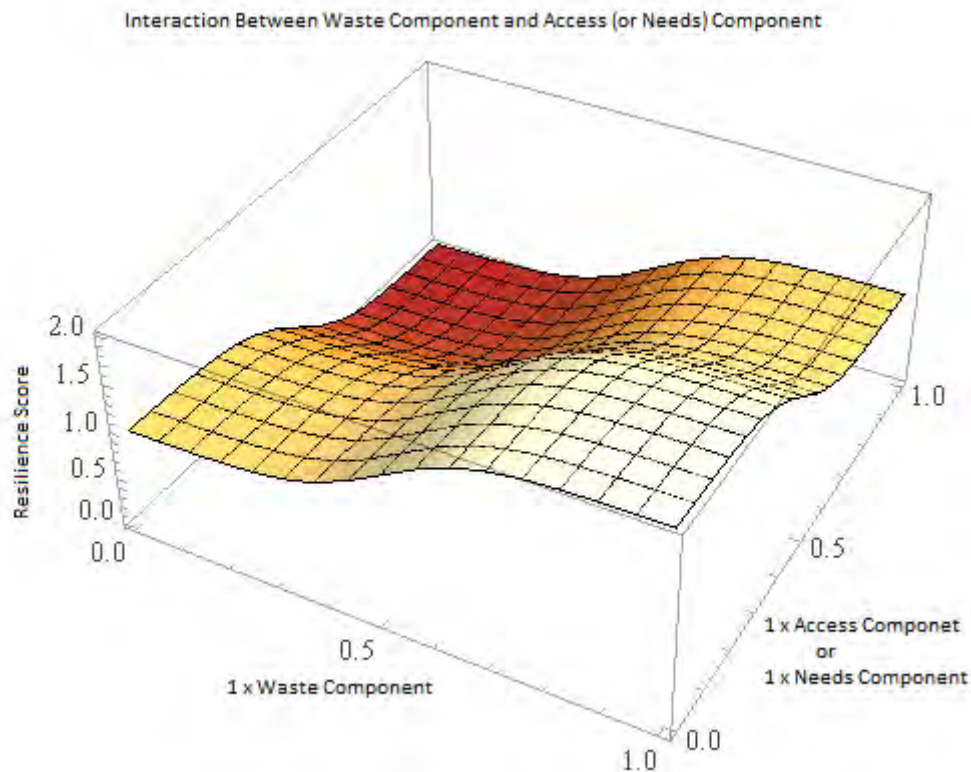


Figure 90: Surface mapping of interaction between a single waste and a single needs/access value

Returning to (14), Figure 91 offers a more nuanced rendering of the interactions between the grouped outputs. Unlike previous graphs, I am rendering a sampling of the possible output values for each of the three components of (14). At the far right, high component scores each contribute to a high score for resilience. It is also read as there exists no, zero, unique knowledge/tasks/resources possessed by pendant agents. There are no knowledge or resource

shortages for any tasks, and there are twice as much knowledge in the organization as assigned tasks need. The opposite end of the graph, at the left, depicts a scenario where there is nothing but unique knowledge and resources possessed by pendants. There are shortages of knowledge and resources for every task, and there is no excess knowledge or resources of any kind in the organization. Such an organization scores a zero (0) in this resilience measure.

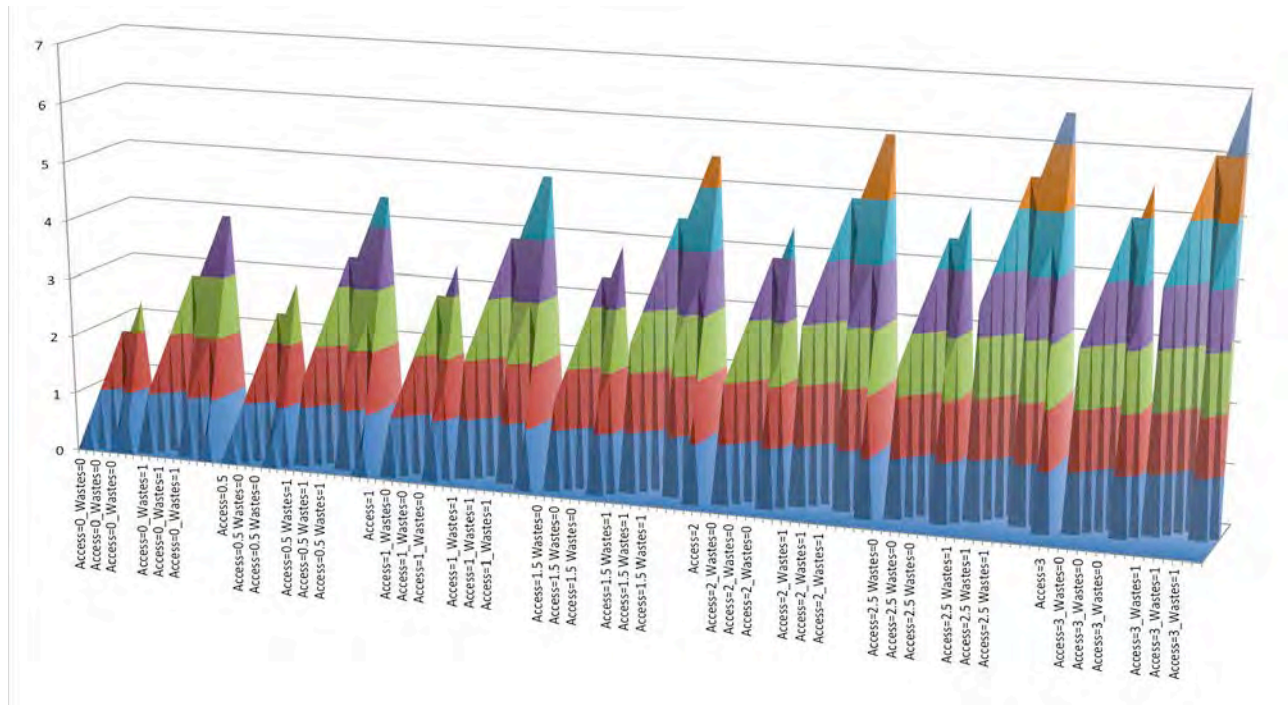


Figure 91: 3D surface rendering of theoretical resilience scores, as function of access indices, wastes, and needs

Resilience indicators for strategic and operational models

We can assess network models of organizations in terms of their structural changes when a node or sets of links leave an organization. Picking the nodes to delete is of course one of challenges and which to pick depends on the task at hand—disruption of information flow or ensuring continued information flow? Breaking a network into segments with a single deletion or multiple deletions and under what constraints? To explore these questions, node-level measures help generate Key Entity reports, thereby reducing the possible deletion pool from the entire model to a more restricted set of nodes. Network-level measures then provide the pool of measures of interests ([Mols](#)) that reflect the effects of IT agents and IT Resource node deletions. Potentially, we are also interested in the changes to node-level metrics for the nodes left behind as well—identifying shifts in node-level metrics for follow-on analysis or action. In light of the above, I present here a list of network measures, their base line values, and discussion points that

can serve as markers of resilience to contested cyber environments. It is likely, in future research, that additional network measures within ORA™ can add to the robustness of analysis and expand the scope of possible disrupting or negative events as well as to-be-developed measures.

Table 26: Dissertation measures of interest (MoI)

Network Measure	Discussion and How/Why it is relevant to assessing resilience in a contested cyber environment¹⁵
Resilience Score	The proposed newest measure seeks to quantify the vulnerability based on scarcity of access to resources, knowledge and tasks. The perception that a entity with few connections to the rest of the model could have significant effects through its absence runs counter to many more traditional modes of social network analysis. It does however mesh with the specialization of functions and roles within modern organizations with broad ranges of responsibilities.
The remainder of the network-level measures are in alphabetical order	
Characteristic Path Length	For each node set, the average path length across all linked nodes in that set. Most relevant to linked human and IT agents that manipulate and process information while performing tasks. The shorter the path, the faster information may flow. Path lengths not perturbed by node deletions indicate resilience to path disruptions. Excessively high path lengths can, though out of scope for this work, indicate room for pruning communications links within an organization.
Congruence, Organization Agent Knowledge Needs	Across all agents, the amount of knowledge needed for completion of assigned tasks, expressed as a percentage of total knowledge needed. Clearly low needs values are more appropriate for organizations than high values.
Congruence, Organization Agent Knowledge Wastes	Across all agents, the amount of knowledge possessed by agents not required by assigned tasks. Wastes, when not substitutable for other knowledge, represent expenditure of cognitive resources by agents that they might otherwise use for the benefit of the organization. Lower values will generally be preferable over high values.
Congruence, Organization Agent Resource Needs	Like knowledge needs, but with respect to resources. Clearly low needs values are more appropriate for organizations than high values.
Congruence, Organization Agent Resource Wastes	Like knowledge wastes, but with respect to resources. Wastes, when not substitutable for other knowledge, represent expenditure of cognitive resources by agents that they might otherwise use for the benefit of the organization. Lower values will generally be preferable over high values.
Congruence, Organization Task Knowledge Needs	Across all tasks, the amount of knowledge lacking to tasks expressed as a percentage of total knowledge needed. Clearly low needs values are more appropriate for organizations than high values.
Congruence, Organization Task Knowledge Wastes	Across all tasks, the amount of excess knowledge to tasks expressed as a percentage of total knowledge needed. Wastes, when not substitutable for other knowledge, represent expenditure of cognitive resources by agents that they might otherwise use for the benefit of the organization. Lower values will generally be preferable over high values.

¹⁵ Unless otherwise noted, definitions and explanations for these measures are verbatim from (Kathleen M. Carley, Juergen Pfeffer, et al., 2012). Discussion of applicability to the dissertation is original work by the author.

Table 26: Dissertation measures of interest (MoI)

Network Measure	Discussion and How/Why it is relevant to assessing resilience in a contested cyber environment¹⁵
Congruence, Organization Task Resource Needs	Like task knowledge needs, but with respect to resources. Clearly low needs values are more appropriate for organizations than high values.
Congruence, Organization Task Resource Wastes	Like task knowledge wastes, but with respect to resources. Wastes, when not substitutable for other knowledge, represent expenditure of cognitive resources by agents that they might otherwise use for the benefit of the organization. Lower values will generally be preferable over high values.
Congruence, Social Technical	The match between the coordination requirements established by the dependencies among tasks and the actual coordination activities carried out by the engineers. In other words, the concept of congruence has two components. First, the coordination needs determined by the technical dimension of the socio-technical system and, secondly, the coordination activities carried out by the organization representing the social dimension (Cataldo, Herbsleb, & Carley, 2008).
Density, Clustering Coefficient	The average of nodes' clustering coefficient. The higher the value the more like a small world network—the more the network supports local information diffusion as well as a decentralized infrastructure.
Diffusion	Computes the degree to which something could be easily diffused (spread) throughout the network. This is based on the distance between nodes— inferred when latitude/longitude data is not available for the Location node set. A large diffusion value means that nodes are close to each other, and a smaller diffusion value means that nodes are farther apart.
Fragmentation	The proportion of nodes disconnected from the network, though not completely isolated. The more fragments in a model, the less likely the network is to diffusion information well, synchronize task execution, or otherwise perform as a purposeful whole.
Isolate Count	The number of isolates in a model. The more isolates in a model, the less likely the network is to diffusion information well, synchronize task execution, or otherwise perform as a purposeful whole.
Overall Complexity	The density of the metanetwork as a whole. Denser network have more links between nodes than less dense networks, usually indicating higher resilience to node removal.
Performance as Accuracy	Measures how accurately agents can perform their tasks based on the agent's access to knowledge required of the tasks.
Social Density	Density of the Agent x Agent network.
Speed	The inverse of the average shortest path length between two arbitrary nodes.
Shared Situation Awareness (Aggregated)	This is usually a node-level and dyad-level measure. However, when aggregated across all agents in a model, it can provide a view of the mean and distribution of the value.

Baseline resilience measures of interest (MoI)

MoI 1: Baseline resilience score

The descriptive statistics below in [Table 27](#) reflect the baseline for each of the D2M models. In this research, the strategic model earned a higher resilience score than the operational. There is insufficient data to speculate on the causation of why the resilience score ordering mimics the ordering of the levels of war. The data below indicates that strategic organizations have substantial knowledge and resources at their general disposal for reacting to negative events—though the measure does not attempt to assess how difficult any adaptations may be.

Table 27: Descriptive statistics for D2M resilience scores

Model	N	Minimum	Maximum	Mean
	Statistic	Statistic	Statistic	Statistic
Strategic	1	5.581919	5.581919	5.5819196
Operational	1	5.087243	5.087243	5.0872437

MoI 2: Baseline characteristic path length resilience score (agent, IT Agent, IT Resource)

ORA™ also labels characteristic path length as averageDistance. The strategic and operational models, as shown in [Table 28](#) have an above average score based on (Kathleen M. Carley & Kim, 2008). This indicates that as modeled, these organizations have a smaller average value for links between arbitrary agents (and IT resources). This score is reflective of the organization's ability to pass information quickly between agents.

Table 28: Descriptive statistics for D2M characteristic path length

Model	Measure	N	Minimum	Maximum	Mean
		Statistic	Statistic	Statistic	Statistic
strategic	averageDistance_agent	1	4.352554	4.352554	4.35255400
	averageDistance_IT Agent	1	5.461147	5.461147	5.46114700
	averageDistance_IT Resource	1	3.489093	3.489093	3.48909300
operational	averageDistance_agent	1	5.198773	5.198773	5.19877300
	averageDistance_IT Agent	1	9.842969	9.842969	9.84296900
	averageDistance_IT Resource	1	4.212481	4.212481	4.21248100

MoI 3: Baseline Congruence, Organization Agent (and IT Agent) Knowledge Needs score

The strategic model is ahead of the operational model for the IT Agents, but behind the operational model for Agents. For both models, agents are less well off than their electronic

peers. The scores for both models indicate that the organizations have significant room for improvement—alternatively it indicates authors of documents about the organizations should be more robust in describing the links between people, technology, and tasks.

Table 29: Descriptive statistics for D2M congruence, organization, agent knowledge needs

Model	Measure	N	Minimum	Maximum	Mean
		Statistic	Statistic	Statistic	Statistic
strategic	congruenceOrgAgentKnowledgeNeeds_task	1	.2422910	.2422910	.242291000
	congruenceOrgIT AgentKnowledgeNeeds_task	1	.5885547	.5885547	.588554700
operational	congruenceOrgAgentKnowledgeNeeds_task	1	.2787664	.2787664	.278766400
	congruenceOrgIT AgentKnowledgeNeeds_task	1	.4187375	.4187375	.418737500

Mol 4: Baseline Congruence, Organization Agent (and IT Agent) Knowledge Wastes score

These scores indicate that agents, IT agents, and roles in the doctrine-defined models have very little knowledge considered ‘waste.’ Waste in this context is knowledge with one or more links to agents, but there is no task that needs the knowledge to which the agents have links. In the context of (14), this corresponds with an output in the waste component of nearly zero (0), also indicating very little resilience to the loss of access to knowledge in the organization.

Table 30: Descriptive statistics for D2M congruence, organization, agent knowledge waste

Model	Measure	N	Minimum	Maximum	Mean
		Statistic	Statistic	Statistic	Statistic
strategic	congruenceOrgIT AgentKnowledgeWaste_task	1	.0443308	.0443308	.044330780
	congruenceOrgAgentKnowledgeWaste_task	1	.0140131	.0140131	.014013100
operational	congruenceOrgIT AgentKnowledgeWaste_task	1	.0409634	.0409634	.040963360
	congruenceOrgAgentKnowledgeWaste_task	1	.0275715	.0275715	.027571470

Mol 5: Baseline Congruence, Organization Agent (and IT Agent) Resource (and IT Resource) Needs score

This Mol contributes to one-third (1/3) of (14) in the needs component of that function. It reflects, across the agents in a network-based model of an organization, the percentage of tasks that lack required resources. The lack of resources does not assure failure of a task, but it does decrease the probability of successful and satisfactory completion. Unlike in [Mol 3: Baseline Congruence, Organization Agent \(and IT Agent\) Knowledge Needs score](#), the strategic model is in second place, behind the operational model in each disaggregated measure. [Figure 92](#) depicts the same information in scatter plot form.

Table 31: Descriptive statistics for D2M congruence, organization, [agent | IT agent] [resource | IT resource] needs, baseline

Model	Measure	N	Minimum	Maximum	Mean
		Statistic	Statistic	Statistic	Statistic
strategic	congruenceOrgAgentResourceNeeds_task	1	.1925941	.1925941	.192594100
	congruenceOrgITAgentResourceNeeds_task	1	.4864685	.4864685	.486468500
	congruenceOrgAgentITResourceNeeds_task	1	.2038859	.2038859	.203885900
	congruenceOrgITAgentITResourceNeeds_task	1	.4391244	.4391244	.439124400
operational	congruenceOrgAgentResourceNeeds_task	1	.5028715	.5028715	.502871500
	congruenceOrgITAgentResourceNeeds_task	1	.6678281	.6678281	.667828100
	congruenceOrgAgentITResourceNeeds_task	1	.9963437	.9963437	.996343700
	congruenceOrgITAgentITResourceNeeds_task	1	.5575537	.5575537	.557553700

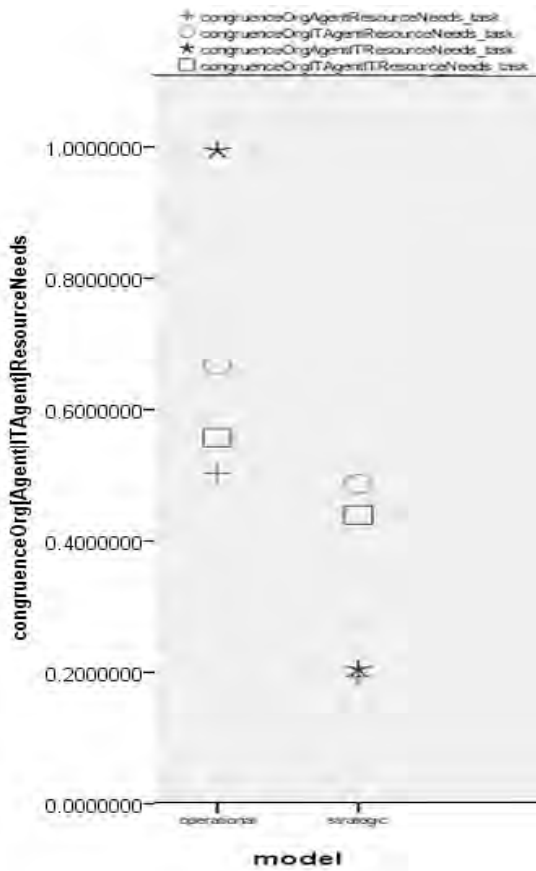


Figure 92: congruenceOrg[agent | IT agent] [resource | IT resource] needs score

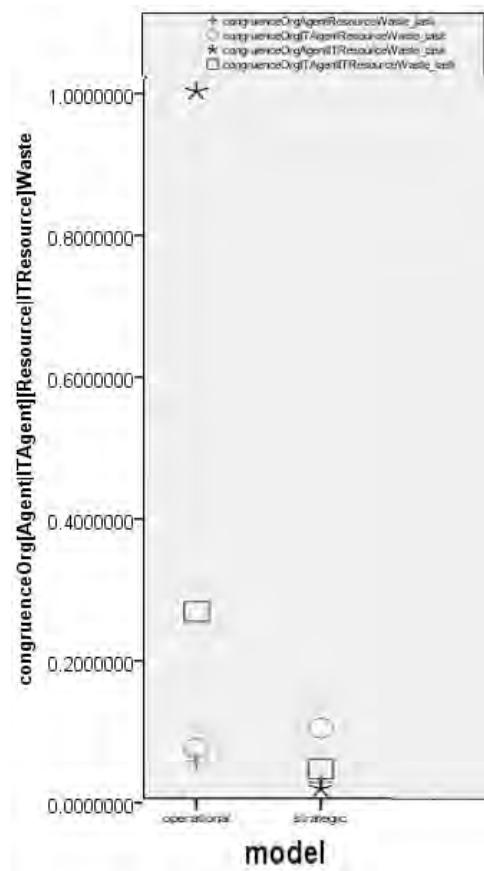


Figure 93: congruenceOrg[agent | IT agent] [resource | IT resource] waste, baseline

MoI 6: Baseline Congruence, Organization Agent Resource Wastes score

This MoI contributes to one-third (1/3) of (14) in the waste component of that function. Figure 93 above, and Table 32 below, reflect the information for this MoI. This MoI, across the agents in a network-based model of an organization, is the percentage of tasks that have access to resources not explicitly required by tasks. The excess resources do not assure an organization of resource substitution or transfer, but they could conceivably increase the probability of successful and satisfactory completion in the event of loss of original resources. Another phrase for excess resources is spare capacity. Spare capacity generally implies substitutability at some reasonable ratio, but the D2M model would rely on the contributing thesauri to help identify words or word phrases to signal that particular level of meaning.

With context however, high scores for ‘waste’ for IT resources and IT agents bode well for any organization in terms of resilience. Without spare capacity, or waste in the more traditional verbiage of DNA, the organization is exhibiting very little ability to absorb or deflect adverse effects caused by a reduction in IT agents’ presence.

The operational model has the highest scores for this MoI with the strategic model barely half as good. The Supply Chain management domain of research would likely assert these low scores reflect a desirable allocation of resources—but with little to no excess resources to support reallocation, leaders have less decision and execution space to operate in.

Table 32: Descriptive Statistics for D2M congruence, organization, [agent | IT agent] [resource | IT resource] waste, baseline

Model	Measure	N	Minimum	Maximum	Mean
		Statistic	Statistic	Statistic	Statistic
strategic	congruenceOrgAgentResourceWaste_task	1	.0227923	.0227923	.022792310
	congruenceOrgITAgentResourceWaste_task	1	.0991865	.0991865	.099186480
	congruenceOrgAgentITResourceWaste_task	1	.0137338	.0137338	.013733750
	congruenceOrgITAgentITResourceWaste_task	1	.0416444	.0416444	.041644420
operational	congruenceOrgAgentResourceWaste_task	1	.0516288	.0516288	.051628760
	congruenceOrgITAgentResourceWaste_task	1	.0709751	.0709751	.070975060
	congruenceOrgAgentITResourceWaste_task	1	.9989119	.9989119	.998911900
	congruenceOrgITAgentITResourceWaste_task	1	.2638718	.2638718	.263871800

MoI 7: Baseline Congruence, Organization Task Knowledge Needs score

From the task perspective, this measure reveals a mixed message for each of the D2M models. The operational model has the least variance between the two varieties of this measure, while the strategic model has the least needs across all the tasks. This measure suggests the strategic organizations modeled are better positioned for completing their tasks as they have fewer knowledge gaps. Fewer knowledge gaps generally correlate to higher rates of task completion as well as higher accuracy for those tasks.

Table 33: Descriptive Statistics for D2M congruence, organization, task knowledge needs, baseline

Model	Measure	N	Minimum	Maximum	Mean
		Statistic	Statistic	Statistic	Statistic
strategic	congruenceOrgTaskKnowledgeNeeds_agent	1	.1067627	.1067627	.106762700
	congruenceOrgTaskKnowledgeNeeds_itagent	1	.3208613	.3208613	.320861300
operational	congruenceOrgTaskKnowledgeNeeds_agent	1	.2940585	.2940585	.294058500
	congruenceOrgTaskKnowledgeNeeds_itagent	1	.2127802	.2127802	.212780200

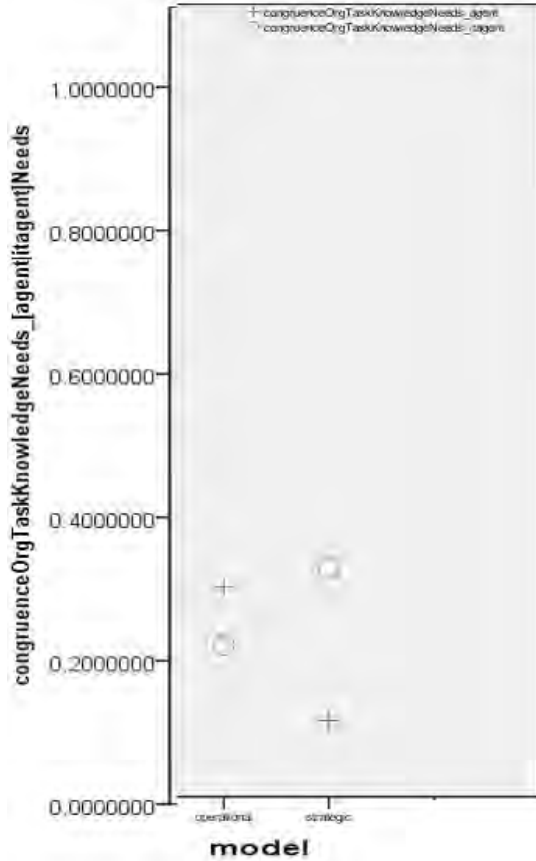


Figure 94: congruenceOrgTaskKnowledgeNeeds, Baseline

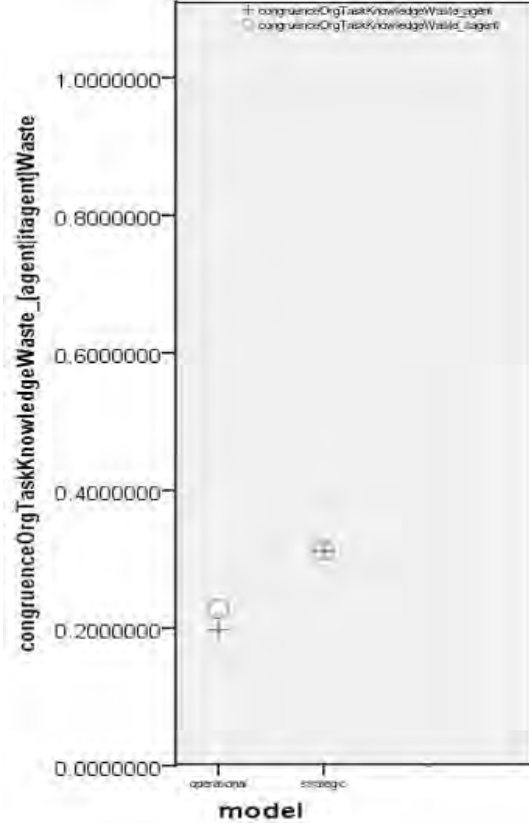


Figure 95: congruenceOrgTaskKnowledgeWaste, Baseline

Mol 8: Baseline Congruence, Organization Task Knowledge Wastes score

From the task perspective, there is an over abundance of knowledge in the models. The D2M models' scores are congruent with what I expected of values in the range of 20-30%. The table below, and [Figure 95](#) above indicate that the strategic model has very low variability between the two varieties but as an organization has a higher waste score than the operational model.

Table 34: Descriptive Statistics for D2M congruence, organization, task knowledge waste

Model	Measure	N	Minimum	Maximum	Mean
		Statistic	Statistic	Statistic	Statistic
strategic	congruenceOrgTaskKnowledgeWaste_agent	1	.3109356	.3109356	.310935600
	congruenceOrgTaskKnowledgeWaste_itagent	1	.3117439	.3117439	.311743900
operational	congruenceOrgTaskKnowledgeWaste_agent	1	.1960738	.1960738	.196073800
	congruenceOrgTaskKnowledgeWaste_itagent	1	.2271573	.2271573	.227157300

Mol 9: Baseline Congruence, Organization Task Resource (and IT Resource) Needs score

Like MOI 8, from the task perspective, this measure reveals a mixed message for the two models. The strategic model has the least variance for the four combinations of this measure. For the strategic model, the IT agents were worse off than regular agents in their needs. This alignment of tasks and resources for the strategic model, and the low starting value for this score, supports a higher resilience score than organizations with large shortages of resources. [Figure 96](#) on the next page and [Table 35](#) below reflect the data.

Table 35: Descriptive statistics for D2M congruence, organization, [agent | IT agent] [resource | IT resource] waste, baseline

Model	Measure	N	Minimum	Maximum	Mean
		Statistic	Statistic	Statistic	Statistic
strategic	congruenceOrgTaskResourceNeeds_agent	1	.1042690	.1042690	.104269000
	congruenceOrgTaskResourceNeeds_itagent	1	.2544663	.2544663	.254466300
	congruenceOrgTaskITResourceNeeds_agent	1	.1094033	.1094033	.109403300
	congruenceOrgTaskITResourceNeeds_itagent	1	.2706257	.2706257	.270625700
operational	congruenceOrgTaskResourceNeeds_agent	1	.4005018	.4005018	.400501800
	congruenceOrgTaskResourceNeeds_itagent	1	.3523277	.3523277	.352327700
	congruenceOrgTaskITResourceNeeds_agent	1	.9986320	.9986320	.998632000
	congruenceOrgTaskITResourceNeeds_itagent	1	.0415371	.0415371	.041537120

Mol 10: Baseline Congruence, Organization Task Resource Wastes score

Unlike Mol 8 and 9, from the task perspective, this measure has a very coherent message for the strategic model compared to the mixed messages for the operational model. [Table 36](#) and [Figure 97](#), below, illustrate the strategic model, like Mol 9, has the least variance for the four combinations of this measure. For the strategic model, it has the least amount of waste, or excess resources for all the tasks in the model. The operational model had all four varieties of this measure above 30% .

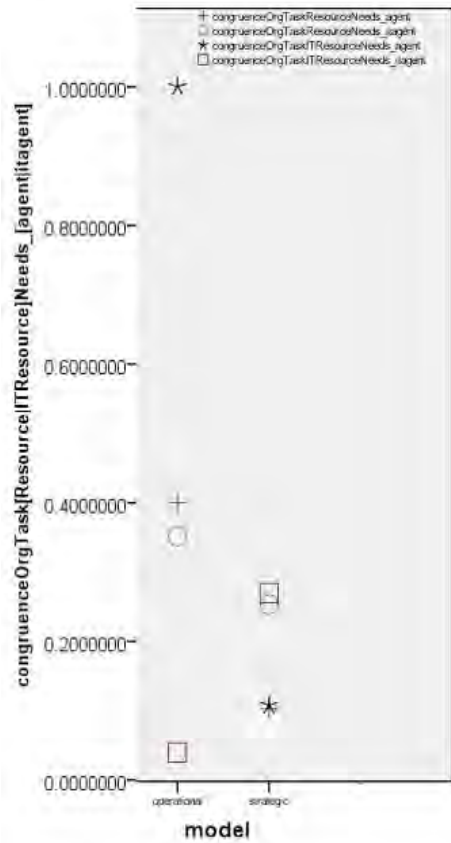


Figure 96: congruenceOrgTaskResource needs, baseline

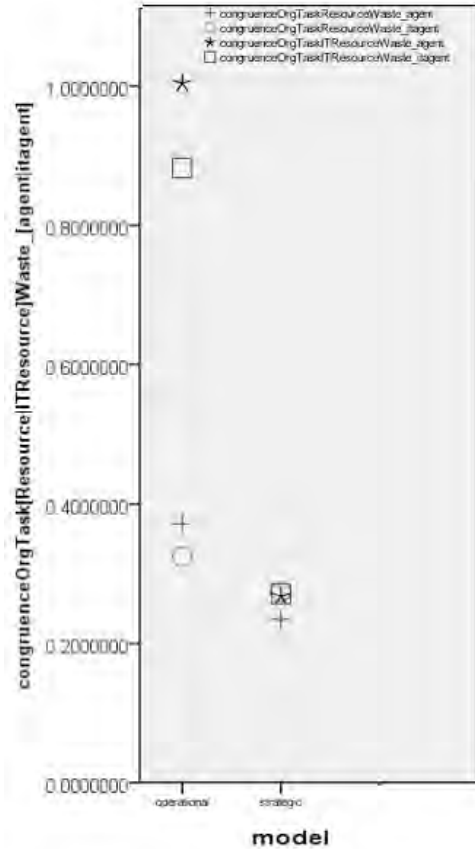


Figure 97: congruenceOrgTaskResource waste, baseline

Table 36: Descriptive statistics for D2M congruence, organization, task [resource | IT resource] waste, baseline

Model	Measure	N	Minimum	Maximum	Mean
		Statistic	Statistic	Statistic	Statistic
strategic	congruenceOrgTaskResourceWaste_agent	1	.2333035	.2333035	.233303500
	congruenceOrgTaskResourceWaste_itagent	1	.2731924	.2731924	.273192400
	congruenceOrgTaskITResourceWaste_agent	1	.2663376	.2663376	.266337600
	congruenceOrgTaskITResourceWaste_itagent	1	.2696142	.2696142	.269614200
operational	congruenceOrgTaskResourceWaste_agent	1	.3698346	.3698346	.369834600
	congruenceOrgTaskResourceWaste_itagent	1	.3228272	.3228272	.322827200
	congruenceOrgTaskITResourceWaste_agent	1	.9999931	.9999931	.999993100
	congruenceOrgTaskITResourceWaste_itagent	1	.8789737	.8789737	.878973700

Mol 11: Baseline Congruence, Social Technical score

On a scale of [0,1], inclusive, this score indicates poor alignment between the assignment of tasks and the social connections needed to gain knowledge to execute those tasks for both models. I had not expected such low scores with these models. An initial hypothesis for why this score would be so low is that doctrinal documents rarely enumerate which particular people use

which particular capabilities and systems to accomplish which particular tasks. The low scores suggest that additional work is necessary to establish how to get the score more congruent with professional opinion in the organizations themselves. It is unlikely that the leaders of the strategic and operational organizations would agree that there is such low alignment between their people and the technology their people need to accomplish their tasks.

Table 37: Descriptive statistics for D2M congruence, social technical

Model	Measure	N	Minimum	Maximum	Mean
		Statistic	Statistic	Statistic	Statistic
strategic	socialTechnicalCongruence_agent_task	1	.01065395	.01065395	.0106539500
	socialTechnicalCongruence_task_itagent	1	.006576661	.006576661	.00657666100
operational	socialTechnicalCongruence_agent_task	1	.00364293	.00364293	.0036429330
	socialTechnicalCongruence_task_itagent	1	.006184001	.006184001	.00618400100

MoI 12: Baseline Density, Clustering Coefficient score

This is a [0,1] scaled-measure, reflected in [Table 39](#) and [Figure 99](#) that assists a leader in learning how similar an organization is to a small-world network. Social network science circles have studied small-world networks and know the networks have very well defined characteristicPlans. One such prominent characteristic is the speed with which such networks of people can pass messages to each other. Given how the military often perceives of itself as a hierarchical organization, I expected these scores to be fairly low. It was somewhat surprising that IT agents and resources were as high as they were. Also surprising was that the strategic model was four times closer to being a small world model than the operational model. I do not have a working hypothesis for the disparity in scores between the two models and defer to future work hypothesizing about the differences.

Table 38: Descriptive statistics for D2M density, clustering coefficient

Model	Measure	N	Minimum	Maximum	Mean
		Statistic	Statistic	Statistic	Statistic
strategic	clusteringCoefficient_agent	1	.21368170	.21368170	.2136817000
	clusteringCoefficient_itagent	1	.227304300	.227304300	.22730430000
	clusteringCoefficient_itresource	1	.408167600	.408167600	.40816760000
operational	clusteringCoefficient_agent	1	.05838165	.05838165	.0583816500
	clusteringCoefficient_itagent	1	.245274800	.245274800	.24527480000
	clusteringCoefficient_itresource	1	.255845000	.255845000	.25584500000

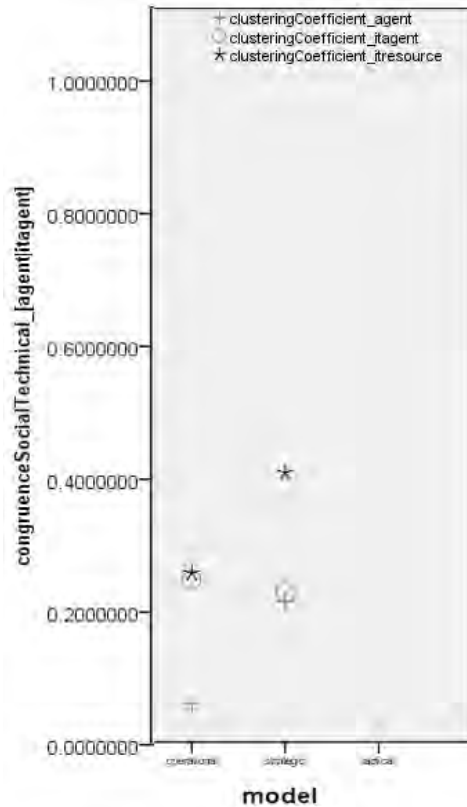


Figure 98: clusteringCoefficient needs, baseline

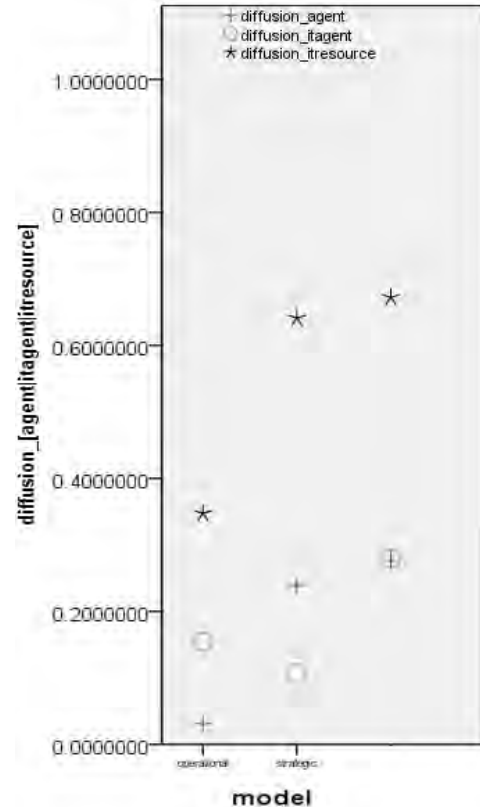


Figure 99: diffusion [it]agent | itresource], baseline

Mol 13: Baseline Diffusion score

Computes the degree to which a network of agents can easily diffuse (spread) something throughout the network. [Figure 99](#) and [Table 39](#) visually depict the diffusion values for both modes. A diffusion value of 1 means that nodes are close to each other. Diffusion, in and of itself, has limited use to leaders attempting to assess their resiliency to adverse events such as contested cyber environments. However, it is a fast measure to calculate, and changes in the measure can support over-time assessment as well as forecasting. For both models, the IT resources seem better positioned for fast message propagation, which would be congruent with expectations of automated message passing.

Table 39: Descriptive statistics for D2M diffusion, baseline

Model	Measure	N	Minimum	Maximum	Mean
		Statistic	Statistic	Statistic	Statistic
strategic	diffusion_agent	1	.2393415	.2393415	.239341500
	diffusion_itagent	1	.10742080	.10742080	.1074208000
	diffusion_itresource	1	.6412405	.6412405	.641240500
operational	diffusion_agent	1	.0312542	.0312542	.031254200
	diffusion_itagent	1	.15454540	.15454540	.1545454000
	diffusion_itresource	1	.3475332	.3475332	.347533200

Mol 14: Baseline Fragmentation score

The proportion of nodes disconnected from the network, though not completely isolated. The more fragments in a model, the less likely the network is to diffusion information well, synchronize task execution, or otherwise perform as a purposeful whole. With this in mind, [Figure 100](#) shows that IT resource fragmentation is the lowest of all three varieties of this measure. Both models' agent varieties earn scores of .70 or higher, indicating a high level of agents not connected to the larger population. The same is true of their IT agents though less so for IT resources.

Table 40: Descriptive statistics for D2M fragmentation, baseline

Model	Measure	N	Minimum	Maximum	Mean
		Statistic	Statistic	Statistic	Statistic
strategic	fragmentation_agent	1	1	1	.76
	fragmentation_itagent	1	.8920292	.8920292	.892029200
	fragmentation_itresource	1	.358133900	.358133900	.35813390000
operational	fragmentation_agent	1	1	1	.97
	fragmentation_itagent	1	.8448566	.8448566	.844856600
	fragmentation_itresource	1	.651077800	.651077800	.65107780000

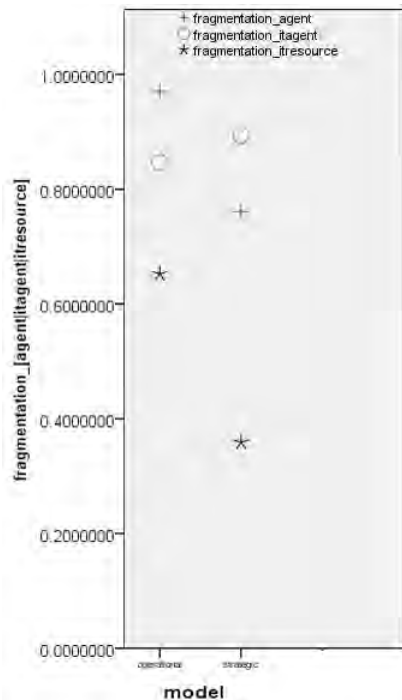


Figure 100: Fragmentation, baseline

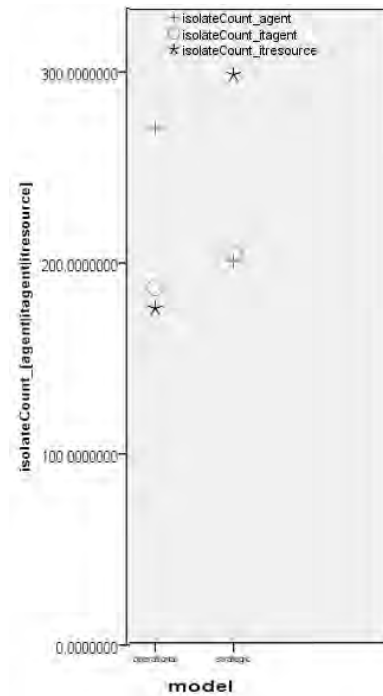


Figure 101: isolateCount [[IT]sgent|resource], baseline

MoI 15: Baseline Isolate Count (Agents, IT agents, and IT resources) score

This measure is a simple count of isolate nodes in a model. The more isolates in a model, the less likely the network is to diffusion information well, synchronize task execution, or otherwise perform as a purposeful whole. These agents did not get deleted during the cleaning processes, as I had chosen to only delete isolates in relation to the entire metanetwork. This means that so long as the agent was connected to any node of any node type, the cleaning process would not delete it. Overall, this is a mixed message across both models.

Table 41: Descriptive statistics for D2M isolate count, baseline

Model	Measure	N	Minimum	Maximum	Mean
		Statistic	Statistic	Statistic	Statistic
strategic	isolateCount_agent	1	201	201	201.00
	isolateCount_itagent	1	205	205	205.00
	isolateCount_itresource	1	299	299	299.00
operational	isolateCount_agent	1	271	271	271.00
	isolateCount_itagent	1	187	187	187.00
	isolateCount_itresource	1	176	176	176.00

MoI 16: Baseline Overall Complexity score

This value is the calculated density of the metanetwork as a whole. Denser networks have more links between nodes than less dense networks, usually indicating higher resilience to node removal among other characteristics. Density, in much the same way as diffusion, is very useful, easy to compute, and changes are easily observed during simulations. Significant changes in complexity are indicators of a change somewhere in the network, the nature of which a leader or researcher would need to exactly determine. In the resilience context, this measure proved less illuminating than expected.

Table 42: Descriptive statistics for D2M complexity, baseline

Model	Measure	N	Minimum	Maximum	Mean
		Statistic	Statistic	Statistic	Statistic
strategic	Complexity	1	.002388317	.002388317	.00238831700
operational	Complexity	1	.002537118	.002537118	.00253711800

MoI 17: Baseline Performance as Accuracy score

Measures how accurately agents can perform their tasks based on the agent's access to knowledge required of the tasks. This is a summary statistic that reflects the general probability that an organization will perform its tasks correctly. Low scores are not good, and while signaling to leaders a misalignment between people, tasks, resources, and knowledge, it does not

identify which particular tasks are more likely to be incorrect than others. [Figure 102](#) and [Table 43](#) depict the scores for the disaggregated collections of human and IT agents, as well as non-IT and IT resources. The operational model shows a higher variability among the groups than the strategic model, but both organizations have lower scores than I expected. These low scores detract from the face validity of the model with respect to this measure. The leaders of the organizations captured in the D2M process would surely disagree that their organizations are getting their tasks and missions done with less than 20% accuracy.

Table 43: Descriptive statistics for D2M performance as accuracy, baseline

Model	Measure	N	Minimum	Maximum	Mean
		Statistic	Statistic	Statistic	Statistic
strategic	performanceAsAccuracy_agent_resource	1	.198872000	.198872000	.19887200000
	performanceAsAccuracy_agent_itresource	1	.184975500	.184975500	.18497550000
	performanceAsAccuracy_itagent_resource	1	.027839	.027839	.02783935
	performanceAsAccuracy_itagent_itresource	1	.028977	.028977	.02897680
operational	performanceAsAccuracy_agent_resource	1	.041837840	.041837840	.04183784000
	performanceAsAccuracy_agent_itresource	1	.060753970	.060753970	.06075397000
	performanceAsAccuracy_itagent_resource	1	.028103	.028103	.02810312
	performanceAsAccuracy_itagent_itresource	1	.037095	.037095	.03709463

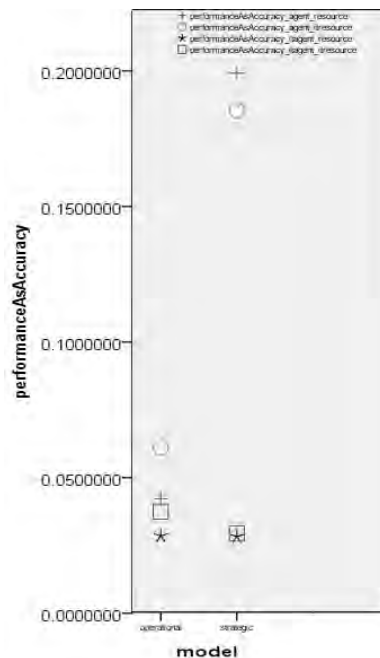


Figure 102: performanceAsAccuracy, baseline

Mol 18: Baseline Social Density score

At the core of every organization are its human resources. This measure captures the density of the known social network(s) as reflected in the links between agent nodes. This dissertation, as a result of disaggregating IT agents from agents, has two flavors of this measure per model. The data in [Table 44](#) indicate a fairly low density for the organizations modeled. A working hypothesis is the doctrine documents need supplementing with more detailed internal SOPs to more closely reflect organizations' self-perceptions.

Table 44: Descriptive statistics for D2M Social Density, Baseline

Model	Measure	N	Minimum	Maximum	Mean
		Statistic	Statistic	Statistic	Statistic
strategic	density_agent	1	.00646176	.00646176	.0064617550
	density_agent_x_itagent	1	.001520241	.001520241	.00152024100
operational	density_agent	1	.00179914	.00179914	.0017991390
	density_agent_x_itagent	1	.001570701	.001570701	.00157070100

Figure 103 Social Density, Baseline

Mol 19: Baseline Speed score

The inverse of the average shortest path length between two arbitrary nodes. The data in [Table 45](#) and [Figure 104](#) both reveal that neither organization is near its theoretical maximum of 1.0. Not unexpectedly, the IT Resources have the highest scores with the human agents coming in noticeably slower.

Table 45: Descriptive statistics for D2M averageSpeed, Baseline

Model	Measure	N	Minimum	Maximum	Mean
		Statistic	Statistic	Statistic	Statistic
strategic	averageSpeed_agent	1	.2297502	.2297502	.229750200
	averageSpeed_itagent	1	.18311170	.18311170	.1831117000
	averageSpeed_itresource	1	.2866074	.2866074	.286607400
operational	averageSpeed_agent	1	.1923531	.1923531	.192353100
	averageSpeed_itagent	1	.10159540	.10159540	.1015954000
	averageSpeed_itresource	1	.2373898	.2373898	.237389800

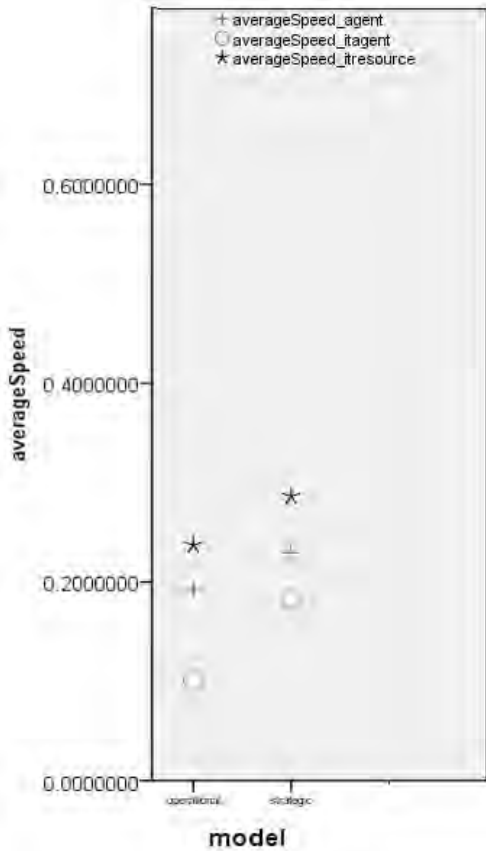


Figure 104: averageSpeed, baseline

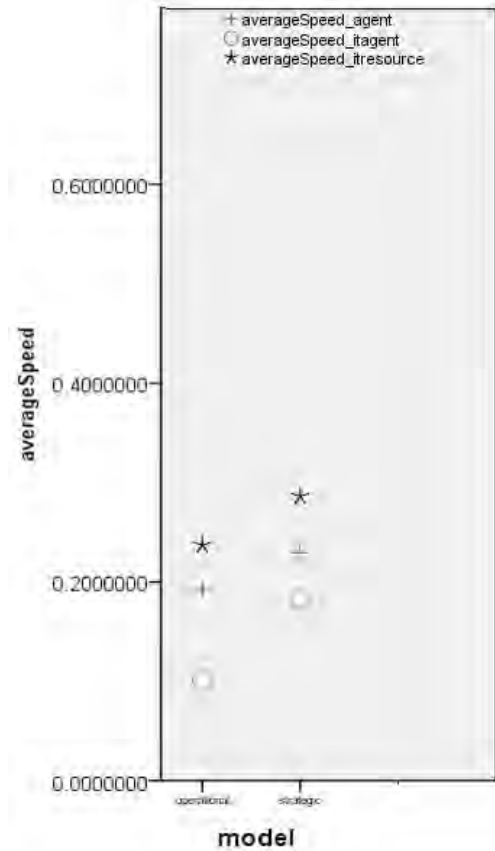


Figure 105: Shared situation awareness (agent and IT agent), baseline

Mol 20: Baseline Shared Situation Awareness score

This is usually a node-level and dyad-level measure. However, when aggregated across all agents in a model, it can provide a view of the mean and distribution of the value. The rendition of this measure is shown below in [Table 46](#) and above in [Figure 105](#). These results were not congruent with expectations and certainly would not be in congruence's with the perceptions of the leaders of the modeled organizations. A working hypothesis is that this measure may be ill suited to this form of model construction, as there are few indicators of actual location—and Graham et al. demonstrated that physical proximity was a large contributor to shared situation awareness {Graham, 2004 #7627}.

Table 46: Descriptive statistics for D2M Shared Situation Awareness, Baseline

Model	Measure	N	Minimum	Maximum	Mean
		Statistic	Statistic	Statistic	Statistic
strategic	sharedSituationAwareness_agent	1	.002326	.002326	.00232558
	sharedSituationAwareness_itagent	1	.001851852	.001851852	.00185185200
operational	sharedSituationAwareness_agent	1	.002532	.002532	.00253165
	sharedSituationAwareness_itagent	1	.001524390	.001524390	.00152439000

The tables above support the original assertions that the ideal information processing resilient organization should have no near isolates, maximal excess knowledge and resources (e.g., twice what is minimally necessary), and no needs. They also show that the least resilient organization is hyper-efficient in knowledge and resource distribution with no waste whatsoever. The least resilient organization also has the degenerate case that all tasks, resources, and knowledge are near isolates and accessible only through agents that are pendants. Finally the least resilient organization has every task short of necessary knowledge and resources. These assessments fulfill the third challenge of organizational leaders: identify their organization's structural vulnerabilities.

The next section begins addressing the fourth challenge for leaders, being able to forecast mission assurance scenarios.

Entropic and Targeted Attacks

ORA™ is capable of performing two types of immediate impact assessments for models to gauge the variability of the resilience indicators in the previous section. The first type is through a replication analysis in which the researcher specifies how many random nodes from which data sets to remove and how many times to run the analysis. This is the entropic attack the heading of this section refers to. ORA™ randomly selects the nodes from among the nodeset (from a uniform distribution), removes the links to/from those deleted nodes, and then recalculates network measures. ORA™ generates the average deltas for the iterations performed.

Previous work (Kathleen M. Carley & Lanham, 2012) indicated that there were minimal impacts (all but one was less than 1% with the one measure changing only 3% from baseline) with random single entity removals. To confirm or refute those findings, I repeated the effort and set the number of entities to randomly remove at one (1), four (4), and ten (10). I had not expected any changes in output measures averaged across multiple repetitions of arbitrary node

removal. The results met my expectations—none of the measures above had any change when recorded across as few as 10 and as many as 1,000 repetitions. This result is most likely due to the sparseness of the various matrices as well as the long right-tailed distribution of link counts between nodes.

The finding above must be emphasized! Small scale random deletions of IT agents in models of information processing organizations rarely have substantial effects. And even in the face of this truism, it is dreadfully wrong for targeted attacks!

For exploratory purposes, and aligned with the Army's Green/Amber/Red/Black color coding of combat capability, I conducted further experiments with random node removal of 15%, 30%, 50% and 75% losses. I also performed a round of deletions at a 90% level. Army doctrine color-codes a unit with up to 15% loss of combat capability as green, up to 30% loss as yellow, up to 50% as red, and anything beyond 50% as black. Of these values, I expected to see high variability in the measures of interest at the 15% level, with significant impacts at the 30% and higher levels. I again started with 10 iterations and spot-checked only a few combinations with 100 replications. None of the measures outputs varied by more than 10% from the baseline until I crossed the 50% threshold, which the Army would consider a 'red' status. The summarized results of the random deletions experiments are below and then operationalized for both the strategic and operational models.

ORA™ executes the second immediate impact analysis using specifically named entity removal in what ORA™ calls impact analysis. In this method, the researcher specifies which nodes to remove from the model, and ORA™ again calculates and depicts the deltas between pre-removal and post removal network measures. This is what I refer to as targeted attacks in this section. Previous work (Kathleen M. Carley & Lanham, 2012) demonstrated nonlinear effects that cross a five percent (5%) threshold change in measures of interest with the top four entities in the Key Entity reports of the IT agents and IT resources. This dissertation revisited this effect by enumerating 1, 4, and 10 nodes for removal. These are clearly significantly fewer than 15% of nodes that I started with in the random targeting—reflective of the difference between random outages and adversaries' efforts to deliberately create significant effects on friendly forces.

To decide which nodes to using in the targeted removal, it is necessary to make a short diversion into what the military calls defended asset lists and prioritized defended asset lists

(PDAL). The next section enumerates an example of a PDAL for each model. I then draw from the PDAL for the targeted node deletions.

Defended Asset Lists and Prioritized Defended Asset Lists

Defended Asset Lists (DALs) and PDALs are, in their simplest incarnations, formal recognition of too few resources for too many demands. Each defensive asset (e.g., anti-aircraft artillery battery, network-based firewall) has finite reach and decreasing effectiveness against varying enemies at varying ranges. With this limitation—often called a limiting factor ([LIMFAC](#)) — in the military, leaders make allocation decisions. Their task is to incorporate a mix of point defenses and area defenses—defending a few things well while balancing the desire to defend ‘everything’ from ‘everything.’ The Air Defense Artillery ([ADA](#)) community, theater missile defense, and strategic missile defense communities are examples of military planners and operations officers who expressly prioritize the importance of the assets they defend. These communities frequently use the [CARVER](#) (Criticality, Accessibility, Recuperability, Vulnerability, Effect and Recognizability) method to provide a quantitative first round estimation that [SMEs](#) then refine and commanders approve. This dissertation’s modeling process can contribute to such efforts by providing another quantitative basis to the decisions of what assets to prioritize based on their position in structural models.

Using this process, without consideration to political, public affairs, or coalition-maintenance considerations, extracts of the PDALs for the three models’ IT resources and IT systems might look like those below. Importantly, though the network analysis identifies key systems, SMEs for each system, the organization itself, and the providers, defenders, and maintainers of the communications methods can, and should, contact and expand the list to include necessary, but unmentioned, supporting technology(ies).

Operational PDALs (IT System and IT resources)

The operational model’s Key Entity reports lead to the contents of [Table 47](#) below. ORA™ provides the seeds for the PDAL and organization SMEs refine the list to ensure the organization maintains the capability. The first such example is internet relay chat (IRC) capabilities—which ranked consistently higher than email. Presuming the IRC servers are not organic to the organization, paths to the servers and terminals to access the IRC servers become

part of the capability on the PDAL in the second column, with comments or other pertinent information in the last column to maintain provenance for the entry.

Table 47: Interpreting key entity reports as a operational PDAL

Primary IT System or IT Resource	Secondary or related IT System or IT Resource	Source / Rationale
IRC Client (NIPR & SIPR)	x terminals (primary and backup) to access IRC server(s)	Key Entity Report
	VLANs and network equipment between IRC terminals and servers	W/o network, terminals are useless
	Primary and backup authentication	W/o login, IRC server unable to allow access
	Firewall rules	Avoid self-inflicted DOS by firewall to local and remote IRC server(s)
	Traffic shaping device and rules	Preserve priority of traffic to local and remote data stores if necessary
JOPES (Joint Operations Planning and Execution System)	x JOPES terminals (primary and backup)	Key Entity Report
	VLANs and network equipment between JOPES terminals and up/downlink(s)	W/o network, terminals are useless
	Primary and backup authentication	W/o login, terminals are useless
	Firewall rules	Avoid self-inflicted DOS by firewall to local and remote data stores
	Traffic shaping device and rules	Preserve priority of traffic to local and remote data stores if necessary
COP (Common Operating Picture)	x COP terminals (primary and backup)	Key Entity Report
	VLANs and network equipment between JOPES terminals and up/downlink(s)	W/o network, terminals are useless
	Primary and backup authentication	W/o login, terminals are useless
	Firewall rules	Avoid self-inflicted DOS by firewall to local and remote data stores
	Traffic shaping device and rules	Preserve priority of traffic to local and remote data stores if necessary
TBMCS (Theater Battle Management C2 System)	x TBMCS terminals (primary and backup)	Key Entity Report
	VLANs and network equipment between TBMCS terminals and up/downlink(s)	W/o network, terminals are useless
	Primary and backup authentication	W/o login, terminals are useless
	Firewall rules	Avoid self-inflicted DOS by firewall to local and remote data stores
	Traffic shaping device and rules	Preserve priority of traffic to local and remote data stores if necessary

GCCS (Global Command and Control System)	x GCCS terminals (primary and backup)	Key Entity Report
	VLANs and network equipment between JOPES terminals and up/downlink(s)	W/o network, terminals are useless
	Primary and backup authentication	W/o login, terminals are useless
	Firewall rules	Avoid self-inflicted DOS by firewall to local and remote data stores
	Traffic shaping device and rules	Preserve priority of traffic to local and remote data stores if necessary
Telephone	x Landline telephone, encryption capable	Leader Directive
	Failure over to non landline	Continuity of Ops Planning
	VoIP satisfactory iff traffic shaping device and rules prevent loss of service	Continuity of Ops Planning
JWICS	x terminals (primary and backup)	Key Entity
	Strategic / permanent link (terrestrial)	Terrestrial links usually have highest bandwidth
	Backup Uplink/Downlink capability	Backup (e.g., TROJAN SPIRIT like capabilities). Continuity of Ops Planning
Other entries as criticality, rehearsed backups/mitigations plans, resources, and other leader-specific criteria dictate		

Strategic PDALs (IT System and IT resources)

The strategic model supports the same analysis though with a different set of capabilities present at the top of the PDAL. For this community the servers, data stores, authentication abilities, intervening firewalls between some defined number of terminals and the supporting servers become part of the package of ‘JOPES’ and ‘GCCS.’ [Table 48](#) expands on the list of ORA™ listed capabilities, with the second column indicating necessary supporting abilities. The third column can provide rationale and continuity of knowledge between shifts and in the face of personnel turbulence.

Table 48: Interpreting key entity reports as strategic PDAL

Primary IT System or IT Resource	Secondary or related IT System or IT Resource	Source / Rationale
JOPES (Joint Operations Planning and Execution System)	x JOPES terminals (primary and backup)	Key Entity Report
	VLANs and network equipment between JOPES terminals and up/downlink(s)	W/o network, terminals are useless
	Primary and backup authentication	W/o login, terminals are useless
	Firewall rules	Avoid self-inflicted DOS by firewall to local and remote data stores
	Traffic shaping device and rules	Preserve priority of traffic to local and remote data stores if necessary
GCCS (Global Command and Control System)	x GCCS terminals (primary and backup)	Key Entity Report
	VLANs and network equipment between JOPES terminals and up/downlink(s)	W/o network, terminals are useless
	Primary and backup authentication	W/o login, terminals are useless
	Firewall rules	Avoid self-inflicted DOS by firewall to local and remote data stores
	Traffic shaping device and rules	Preserve priority of traffic to local and remote data stores if necessary
COP (Common Operating Picture)	x COP terminals (primary and backup)	Key Entity Report
	VLANs and network equipment between JOPES terminals and up/downlink(s)	W/o network, terminals are useless
	Primary and backup authentication	W/o login, terminals are useless
	Firewall rules	Avoid self-inflicted DOS by firewall to local and remote data stores
	Traffic shaping device and rules	Preserve priority of traffic to local and remote data stores if necessary
GAMSS (Global Air Mobility Support System)	x GAMMS terminals (primary and backup)	Key Entity Report
	VLANs and network equipment	W/o network, terminals are useless

	between GAMSS terminals and up/downlink(s)	
	Primary and backup authentication	W/o login, terminals are useless
	Firewall rules	Avoid self-inflicted DOS by firewall to local and remote data stores
	Traffic shaping device and rules	Preserve priority of traffic to local and remote data stores if necessary
Telephone	x Landline telephone, encryption capable	Leader Directive
	Failure over to non landline	Continuity of Ops Planning
	VoIP satisfactory iff traffic shaping device and rules prevent loss of service	Continuity of Ops Planning
JWICS	x terminals (primary and backup)	Key Entity
	Strategic / permanent link (terrestrial)	Terrestrial links usually have highest bandwidth
	Backup Uplink/Downlink capability	Backup (e.g., TROJAN SPIRIT like capabilities). Continuity of Ops Planning
Other entries as criticality, rehearsed backups/mitigations plans, resources, and other leader-specific criteria dictate		

Targeted Assets

The next three tables ([Table 49](#) to [Table 50](#)) list the nodes to remove during the targeted removal conditions of testing. The key entity reports provide these agents as a fast and justifiable listing of nodes that will be likely to inflict disruption on the owning organization(s). The deliberate targeting of capabilities on the PDAL and in the Key Entity report supports measuring the impacts of such removals—large impacts to the chosen measures of interest support the original forecasting.

Table 49: Operational model nodes to Remove

Total Nodes to Remove	Node Title	Node Set
1	Internet Relay Chat (IRC)	IT agents
4	IRC	IT agents
	Joint Operations Planning and Execution System (JOPES)	IT agents
	Joint Warfighter Intelligence Communications System (JWICS)	IT Resource
	Defense Special Security Communications System (DSSCS)	IT Resource
10	IRC	IT agents
	JOPES	IT agents
	Common Operating Picture (COP)	IT agents
	Tactical Battle Management Command and Control System (TBMCS)	IT agents
	Global Command and Control System (GCCS)	IT agents
	Joint Warfighter Intelligence Communications System (JWICS)	IT Resource

	Defense Special Security Communications System (DSSCS)	IT Resource
	World Wide Web (www)	IT Resource
	Global Positioning System (GPS)	IT Resource
	Combined Enterprise Information Exchange System (CENTREX)	IT Resource

Table 50: Strategic Model Nodes to Remove

Total Nodes to Remove	Node Title	Node Set
1	Joint Operations Planning and Execution System (JOPES)	IT agents
4	JOPES	IT agents
	Common Operating Picture (COP)	IT agents
	Joint Warfighter Intelligence Communications System (JWICS)	IT Resource
	Defense Special Security Communications System (DSSCS)	IT Resource
10	JOPES	IT agents
	Common Operating Picture (COP)	IT agents
	Global Command and Control System (GCCS)	IT agents
	Army Data Distribution System (ADDS)	IT agents
	Global Air Mobility Support System (GAMSS)	IT agents
	Joint Warfighter Intelligence Communications System (JWICS)	IT Resource
	Defense Special Security Communications System (DSSCS)	IT Resource
	Army Air Ground System (AAGS)	IT Resource
	Army Tactical Communications Systems	IT Resource
	Common Ground Station (CGS)	IT Resource
	Directory services	IT Resource

Results of entropic and targeted IT agents and IT Resource deletions

Overall, the entropic results confirm the previous work—random attacks against IT assets (systems or resources) have to rise to 30% or more of named assets to have effects on measures of interests that consistently cross a 10% change from baseline threshold. In the context of military battle damage assessment (BDA), for the twenty MoIs in use above, IT causalities have to rise to nearly a ‘red’ level for the effects of their total loss to move from ‘green’ to ‘amber.’ This broad result stands in stark contrast to the expansive statements of impending peril in the mass media.

However, broad results frequently have variability and nuance not well captured in sound bites or single sentence summaries. I will review the nuances of each of the measures of interest in the figures below. Each figure depicts in bar chart format the entropic deletion of nodes, replicated 20 times for each model. The heights of the bars are the percentage change from the baseline values discussed in the previous section. The color-coding matches previous color coding with blue representing the operational model and purple the strategic model. The height

of the like-colored lines represents the percentage change in the targeted node removals for each model. The X-axis has dual labels, with the integers representing the number of nodes removed and the percentage value representing the percentage of the IT agents and IT resource node set population removed.

The first MoI to check is the new measure of resilience.

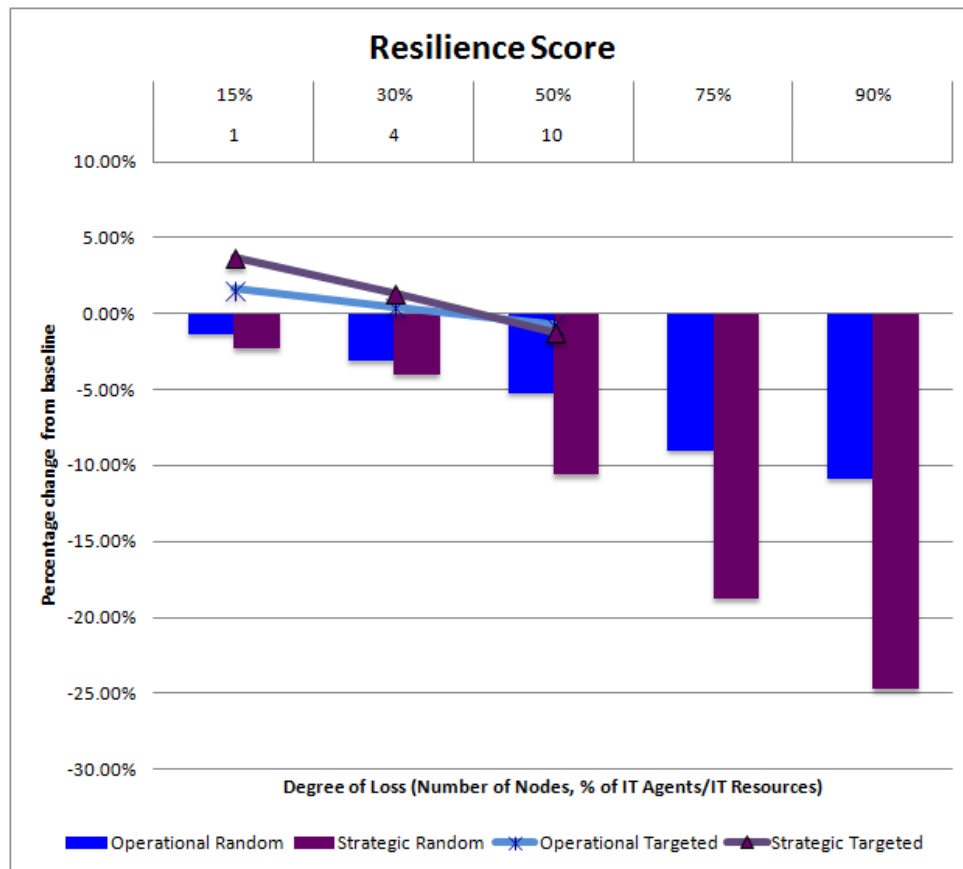


Figure 106: Resilience score for entropic and targeted deletions

The first two MoIs are the Characteristic Path Length and the Communication Speed of IT agents, [Figure 107](#) and [Figure 108](#) respectively. These MoIs are the inverse of each other so a discussion of both at the same time is appropriate. As none of the node removals involved the other node sets, there were no observed changes in this measure for any of the other networks in the model. As I expected, the targeted removal of small numbers of nodes in 600-1,000 node networks, did not in these models, nor is it likely in other models, have significant effects when aggregating at a network level. It is extremely interesting to note however that the removal of as few as ten (10) well-chosen nodes can have an effect as large as removing 50% of the IT agents

and IT resources. As noted in numerous other studies, this effect is clearly the result of the degree distributions of the underlying networks—power-law distributions are resilient to random removals but highly susceptible to removal of hub nodes. With random outages (both self-inflicted and others) being far more common than targeted outages, there is very little wonder so many organizations perceive they can handle deliberate outages when they extrapolate from random outages. A key take away from these two models, and the previous work of (Lanham, Morgan, et al., 2011e), is that a few well chosen IT targets can generate the same effects as the loss of 30% of IT resources for IT related MoIs.

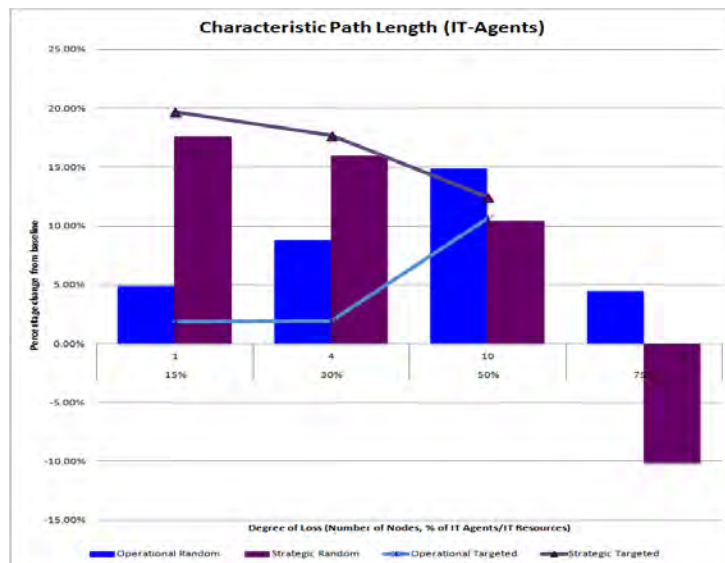


Figure 107: Changes in characteristic path length of IT agents for entropic and targeted deletions

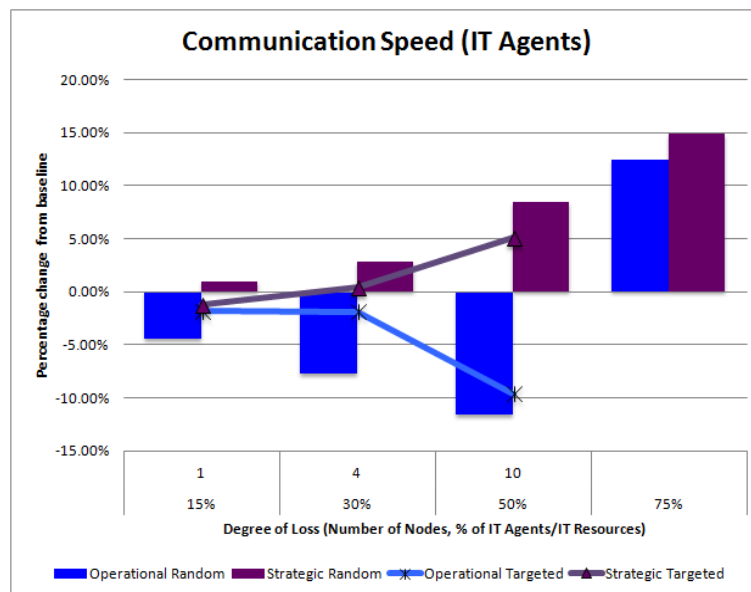


Figure 108: Changes in communication speed of IT agents for entropic and targeted deletions

The next three MoIs paint very similar pictures in the effects at the IT system level. They all show the same pattern: targeted node removals yield results of similar magnitudes with an order of magnitude fewer removals than random attacks. The Density Clustering Coefficient in [Figure 109](#), indicates that both models' IT agents populations move further and further away from a small-world topology. The implication of this finding is that these IT systems will find it harder and harder to move messages between each other. This finding is not reflective of underlying technology protocols that support rerouting of information across operational links (e.g., EGRP or BGP in IP-based routers).

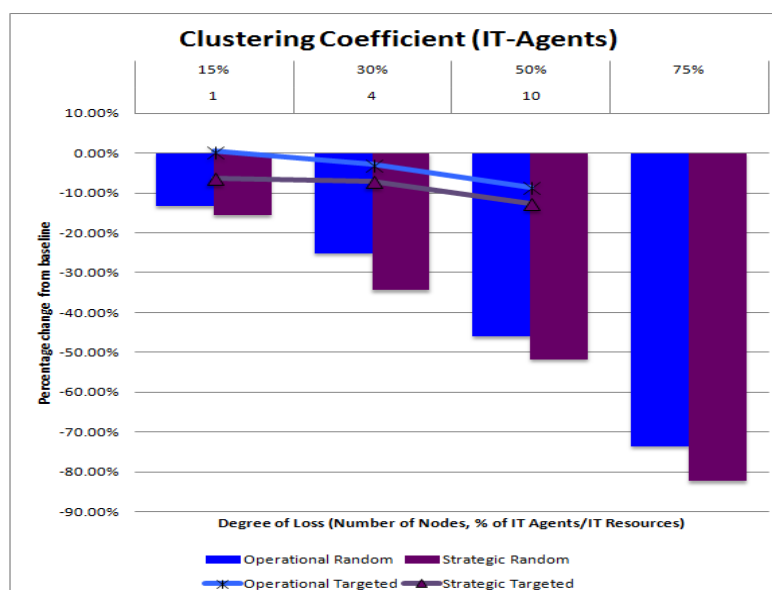


Figure 109: Changes in clustering coefficient of IT agents for entropic and targeted deletions

A related MoI is Diffusion. Diffusion typically requires a location node set inclusive of latitude and longitude (lat./long) information per location. When lat./long data is not present, ORA™ inference distances between agents by calculating and using geodesic distances instead—that is how far apart nodes are by hop count and link weight. In [Figure 110](#), both models display a slightly nonlinear slow down in diffusion as the number of random and targeted nodes deletions goes up. Whether such diffusion slow down is significant for the organization is, of course, context dependent. The general finding should give pause to any leader tasked with working through and recovering from contested cyber environments.

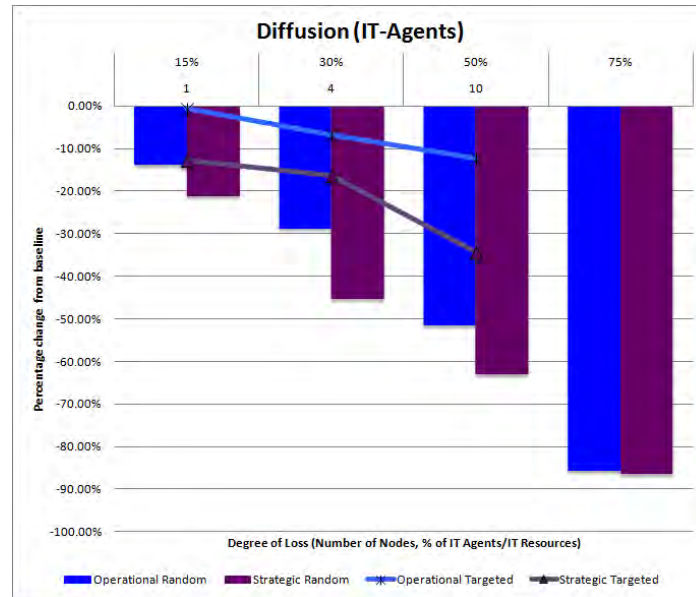


Figure 110: Changes in diffusion of IT agents for entropic and targeted deletions

The third of these related MoIs is Fragmentation and is shown in [Figure 111](#). Here the pattern remains the same—increasing fragmentation as nodes get deleted. What stands out as prominent however is that the operational level organizations are more susceptible to IT system fragmentation than the strategic organizations. I had expected the reverse based on the professional observation that strategic IT systems are highly dependent on free-flowing information and they would be more vulnerable to system deletion and information disruption. One possible explanation could be that the strategic model had a high fragmentation score in the first place. It is reasonable to presume it's hard to fragment an already fragmented network.

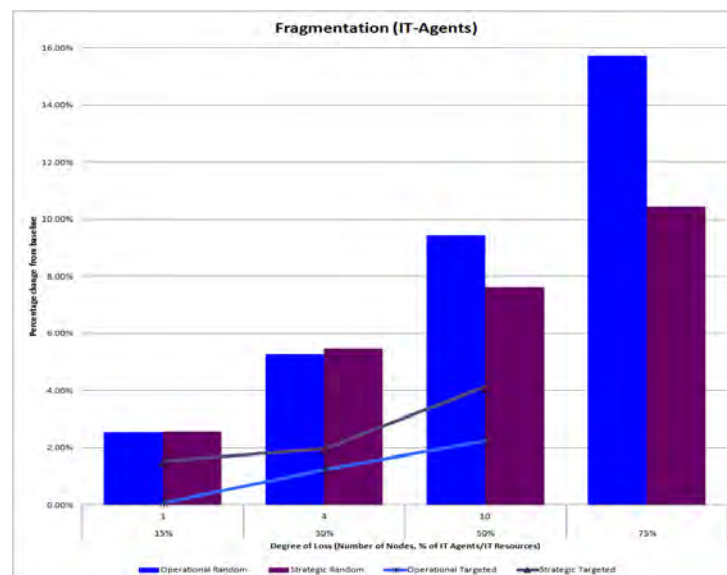


Figure 111: Changes in fragmentation of IT agents for entropic and targeted deletions

The next MoI, Isolate Count, behaved counter to expectations as seen in [Figure 112](#), though a reasonable explanation is not difficult to find once faced with the modeled results. Intuition would suggest that the loss of IT agents and IT resources would lead to increased isolation of other, dependent systems. Results of random deletions however, as shown in [Figure 112](#), lead to fewer isolates within the IT agents x IT agents network, not more. As noted earlier in this chapter, the IT agents node set, when examined in isolation, has 70 to 200 isolates for the tactical through strategic models. When examined within the entire metanetwork context however, the nodes are not isolates but connected to other node types. Given the high fragmentation rating for each model, it is no longer surprising that high quantities of random deletions would serve to reduce the over number of IT agent isolates. It is noteworthy that the targeted deletion of nodes had precisely the expected result, the increasing numbers of isolates!

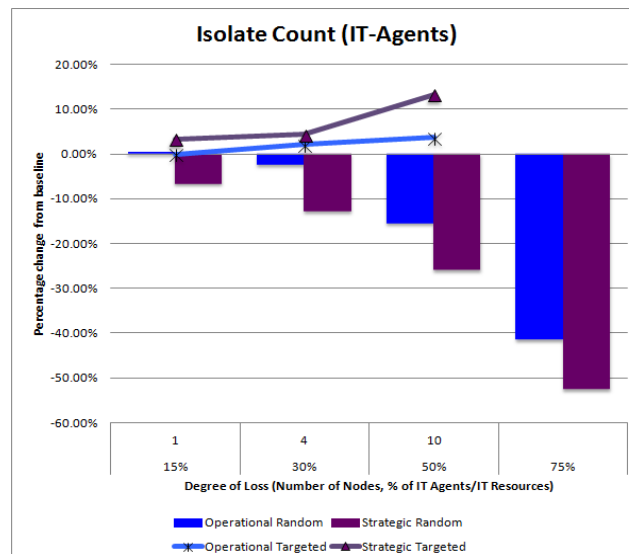


Figure 112: Change in isolate count of IT agents for entropic and targeted deletions

None of the changes in Overall Complexity, [Figure 113](#), rose above 4.5% change from baseline. These are large metanetworks with very low starting densities for each model. I had expected all deletions to lower the density, as with node deletion I expected link deletion. I had failed to incorporate the link distribution into my initial assessment and the results are visible in [Figure 113](#). Random deletion is clearly deleting far more fragmented and low link count nodes, actually improving the over-all density, though the reader may recall the density improvement is insufficient to reduce the characteristic path length until 75% of the IT agent and IT resource nodes are deleted. The changes to the density with the targeted removal are in line with expectations both in the general trend and the magnitude of the decrease.

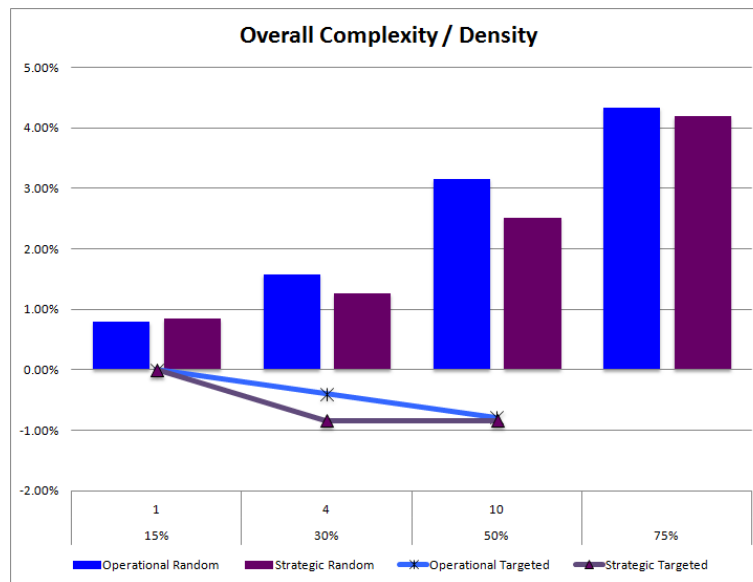


Figure 113: Overall changes in complexity

A more granular examination of density leads us a discussion of Social Density of IT agents—the network density of the IT agents x IT agents network in isolation from the metanetwork as a whole. In this MoI, [Figure 114](#), we see that when focusing on the node set which is applicable to this MoI, there are, again, nonlinear results that differ dramatically by model. Random deletion is clearly not having much effect, with the high fragmentation values for each model. This type of variability and nuance is precisely what is lost in much of the opening paragraphs of related cybersecurity literature. IT specific effects may be significantly different than results aggregated across multiple viewpoints.

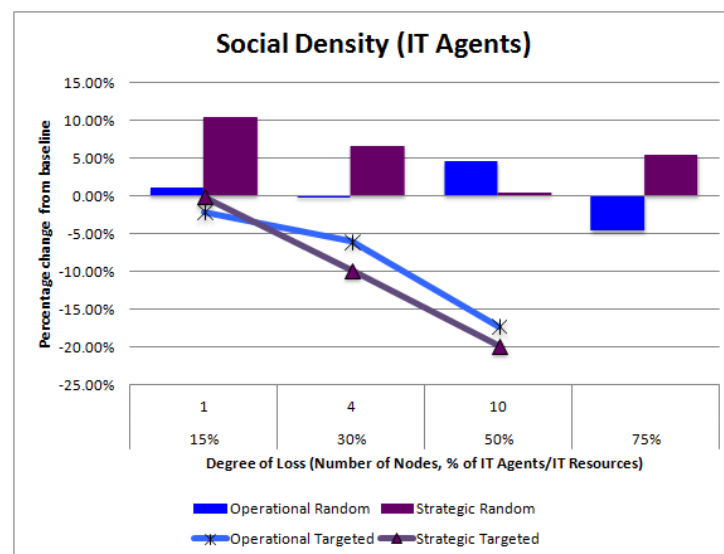


Figure 114: Change in social density of IT agents

The last MoI of this chapter is by far the most interesting and one with interesting variability. Performance as Accuracy is a measure I applied to three node sets in each model: agents, IT agents, and roles. In that order, I'll discuss the findings of the static targeted and entropic node removal impact analysis. When considering just the human agents as problem solvers, there were essentially no effects in the targeted and entropic deletion efforts—no model nor deletion condition led to changes larger than 6% from baseline! As seen in [Figure 115](#), the strategic model had improvements as we deleted random IT agents and IT resources, as did the tactical model and the operational model with one exception. This result may not generalize to all organizations with perceptions of IT dependence—it certainly is counter to numerous public assertions that the American military could be paralyzed by a cyber attack. Even the targeted deletions have very little effect, and not consistently negative either. This too was counter to expectations, but reinforcing earlier work! Though worthy of exploration in live exercises and events, it is possible that far more task knowledge and situation knowledge exists with people in these organizations than the cyberthreat-focused analysts give credit for.

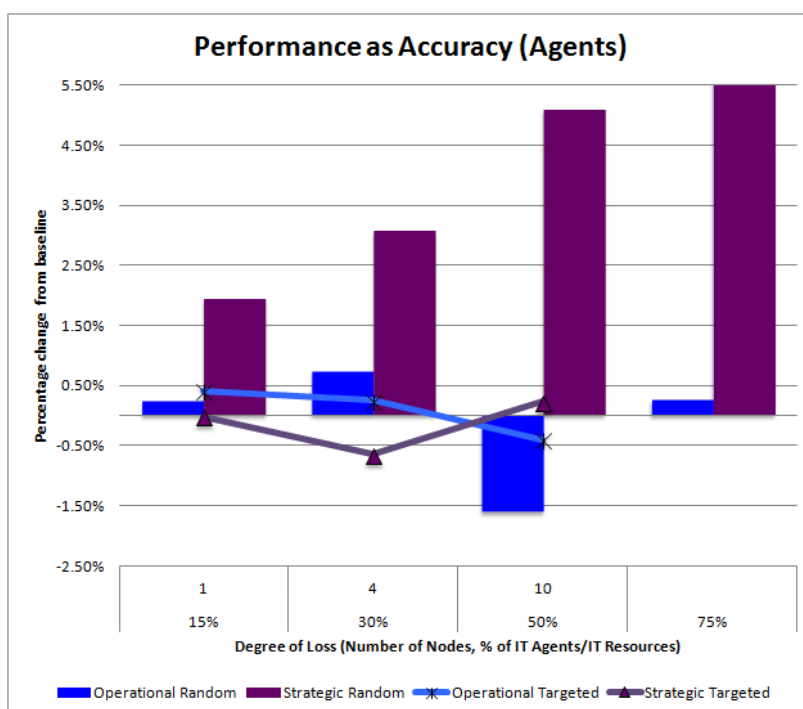


Figure 115: Changes in performance as accuracy of agents

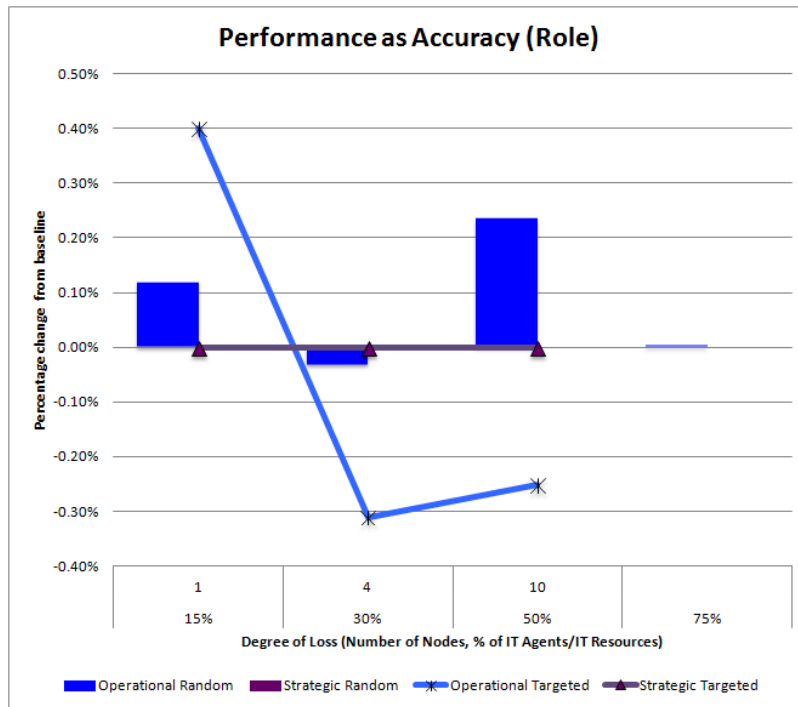


Figure 116: Changes to performance as accuracy of roles

When using the rapid model construction process of this dissertation, and the D2M model in general, one of the output node sets is ‘Roles.’ This node set consists of generalized positions filled by more than one person, so broadly discussed it does not easily map to a single person. These kinds of entities are frequently in doctrine documents or other organizationally generated documents. As such, it is appropriate to examine the impact of removing access to IT agents and IT resources on these types of organizational members. As shown in [Figure 116](#), the impacts are mixed and do not present a clear picture. The impacts are consistently low (all below 1% change from baseline) and as such it is unwise to overly generalize the results both within the two modeled organization types as well into organizational resilience to contested cyber environments.

When disaggregating IT agents from other agents, [Figure 117](#), the impacts of entropic deletions correspond almost exactly with the color coding scheme of the Army: 15% loss of systems equates to approximately 15% loss of accuracy and the consequent color-coding change from Green to amber/yellow. Likewise a 50% loss of random systems equates to a 50% drop in accuracy, moving from yellow to red, and bordering on black. Across these three models, and one other model from previous work, there is now an established trend that random loss of

availability of IT systems and IT resources may not have overt large-scale effects unless the loss crosses a leadership-defined threshold.

Importantly though, the same trend exists for targeted losses, to which organizational leaders must pay very close attention. Loss of Key-Entity-identified-systems, when combined with each other, rapidly causes nonlinear results in very small quantities! In these models, the loss of four capabilities (two (2) IT agents and two (2) IT resources, without expressly considering the mechanisms for their loss) causes the same drop in this MoI as the loss of 15% of the original node populations (see also node populations in [Table 19](#)). In these models, deletion of as few as ten (10) nodes, when carefully selected, can create effects as large as a random loss of 50% of the nodes.

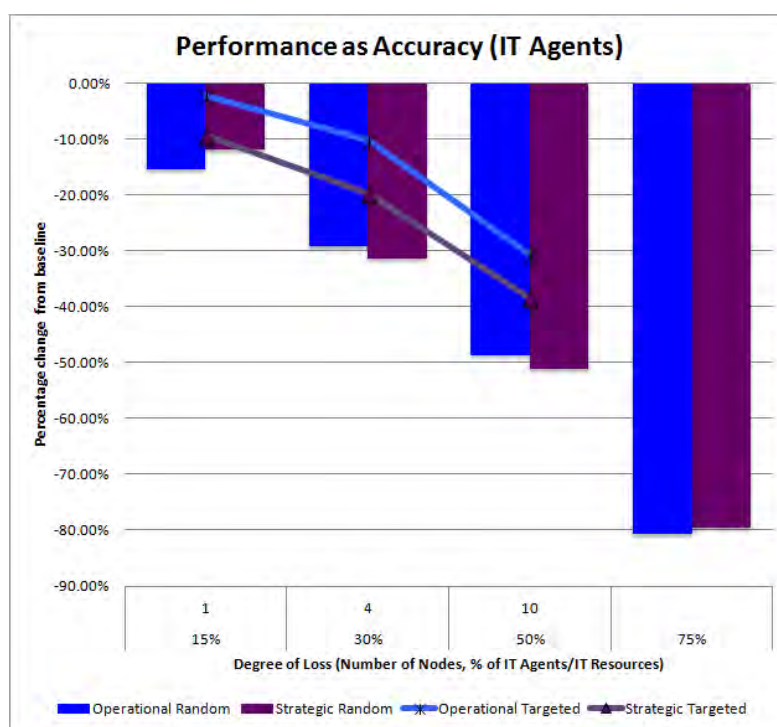


Figure 117: Changes to performance as accuracy of IT agents

Conclusions

In the abstract and Introduction chapter, I listed four demands leaders should place on their organization to increase mission assurance in contested cyber environments. This chapter has addressed the first and third of those four demands: 1) require assessments be more than analogical, anecdotal or simplistic snapshots in time and 3) identify their organization's structural vulnerabilities.

Fundamentally assessments are essential for leaders to have confidence in their ability to maintain their essential missions in contested cyber environments. To conduct assessments, leaders and analysts must start with one or more baselines—this chapter is the baseline for comparison of future time points. With this baseline, and with appropriate questions and measures of interest, leaders and researchers can use M&S to forecast mission assurance scenarios (the fourth demand I listed in the abstract and introduction).

This chapter has demonstrated the application of existing social network analysis and metanetwork analysis measures against two doctrine generated models. The chapter has introduced and demonstrated the calculation of a new metric that takes into account the specialization of organizational functions and components. This measure is a weighted function of the near isolation of tasks, resources, and knowledge, over-supply of knowledge and resources to organizational tasks as well as shortfalls of the same. The new measure assists decision makers through adding an additional dimension of resilience through redundancy of capabilities as well as redundancy of access to capabilities—it does not provide a single ‘magic number’ that can signal “All is well” or “Brace for impact.”

The most important take away from this chapter is that the rapid modeling process of the previous chapter can generate a model subject to analytic efforts that demonstrates a recognizable, though nonunique, outcome: targeted removal of IT systems and IT resources in complex sociotechnical organizations can lead to effects disproportionate to the number of directly affected systems and resources. This trend leads to a lesson for organizational leaders that the risk management community has incorporated for a very long time: identify the most important systems and resources and ensure their continuity of operations at some *a priori* acceptable level.

Organization leaders can use the processes in this chapter to establish contingency plans for their people, organizations, and systems. Offensive targeting can use this process to identify combinations of systems that generate higher payoff than attackers might otherwise achieve. The key is the realization that a few well-chosen losses will predictably have outsized impacts! This phenomenon has earned the moniker ‘black swan event’ in some circles though it is by no means the only descriptor.

In the next chapter, I move from this chapter's point-in-time assessments to a forecasting methodology using D2M derived models and cognitive agent based simulations. Forecasting how organizations adapt to a contested cyber environments can be a useful tool for leaders to use in what-if scenarios and general-purpose cyber resilience discussions.

“All models are wrong, but some are useful,” (Box, 1979)

Agent Based Models and Modeling

This chapter of the dissertation will review related agent based model ([ABM](#)) work in sociotechnical systems and cyber security research. I will also provide a brief discussion of how the [CASOS](#) ABM capability called Construct (Frantz & Carley, 2007; B. Hirshman et al., 2011) operates. These set the stage for a detailed discussion of model preparation and experimental design that I use to demonstrate the resiliency score over time as well as the other indicators of resilience performance.

In brief, the experimental scenario applied to two (2) empirically based models derived from the models discussed in the previous two chapters. In addition to baseline conditions (no attacks of any variety), the experiments involved creating and assessing the effects of cyber attacks in the form of integrity and availability attacks aimed at specific systems, a generalized confidentiality attack, and availability attacks aimed at communications infrastructure between agents. I expected, and simulation experimentation confirmed, varying effects on selected network measures discussed in the last chapter. Importantly, the scenario then added four possible mitigations to the simulation to assess their efficacy—and demonstrating in simulation that networked organizations can adapt to misfortune and assure leadership of their resilience.

The operational scenario for each model was based on the first few steps of the military decision making process ([MDMP](#)): receive a plan and conduct a cycle of mission analysis/planning and briefing of leadership. These steps are, under different names, nearly identical in all organizations tasked with receiving direction from others, planning how to implement those directions, communicating the plan to subordinates, and executing the plan. I represented the operations order ([OPORD](#)) by adding, exogenously, a set of ‘plan’ bits to the set of knowledge bits the D2M process had discerned. I assigned these ‘plan’ bits to the key IT Agents identified using key entity reports. The agents linked to the agent group named “joint planning group” had the task to plan amongst each other (e.g., interact with each and exchange information) then brief organization leadership 3 times during the first one-third of the simulation time. I also added a set of ‘bad plan’ bits for use by the attacking integrity agent. Using a Box-Behnken Response Surface Modeling design, I varied the probability of effects of

each of the six attacks vectors, as well as four mitigation efforts, for a total of ten quantitative variables.

The cyber losses, when enabled, occur during the midst of the plan-brief-plan-brief cycle. I expected, and the simulations experimentation confirmed effects dependent on the probability of effect, the mitigation in place (if any), and the speed with which the mitigation is put in place.

Agent based models and sociotechnical systems

ABMs are ideally suited for developing theories of and exploring via simulations, situations where the modeled entities, as individuals, must perceive and react to their modeled environment(s). When those situations are not conducive to human-subjects studies, simulations using agents help bridge gaps between theory in isolation, theory based on extrapolation from human-subjects studies, and being unable to pursue resolutions to research questions of interest.

ABMs are not the only method of modeling for these situations, as previously discussed in the related literature portion of the dissertation. When the question at hand is continuous flow or process related across well-defined paths, dynamic systems may be a more appropriate vehicle for developing theories of flow (Borshchev & Filippov, 2004). When questions at hand have no interest in forecasting the effects of multiple individuals' actions in an artificial landscape, abstracting the individuals away into sets of equations, sources, sinks, and interference patterns may be a better approach for a researcher. When a researcher wants to study aggregations of entities (e.g., organizations) free from cognitive limitations, there is unmistakably no need to complicate their abstraction with per-entity limitations, or even low-level entities at all! Of course, ABM offers exactly the opportunity for low-level decisions, behaviors, and observables to, without *a priori* rule writing, discover explanatory mechanisms for what appear as deliberate or purposeful crowd-level phenomena. Indeed, a key aspect of a properly designed and built ABM experiment is to ensure that whatever constraints and impulses do exist in the model, they are not artificially driving the result to an aggregate-level outcome through over-controlling the agents (J. H. Miller & Page, 2007).

Examples of ABM use applied to questions of aggregated-level phenomena include theorizing about which organizational designs cope better with communication breakdowns at agent levels (Kathleen M. Carley, 1991; DHS, 2011). OrgAhead is another example of ABM used to improve patient care at the unit-level (Effken et al., 2005), evaluate team performance in

the face of turnover when interactions include face-to-face as well as technology-enabled mechanisms (Levine, Moreland, Argote, & Carley, 2005). Indeed Levine's work, using a code-base predecessor of Construct, validated the results of the ability to generate realistic patterns of behavior among artificial agents as well as generated aggregated results congruent with human-subject experiments. Canessa's work using ABM was another effort at demonstrating replication of emergent behavior from collections of agents interacting with and without the aid of technology (Canessa & Riolo, 2003). That work also demonstrated structure/network-based effects mediated by technology as well as the effects of out-of-group forced interactions on intra-group performance. The breadth of examples of researchers using ABM to help build and test theories is well beyond the scope of this dissertation to cover. What is notable however are the research areas between these examples of ABM applied to sociotechnical systems and current incarnations of cybersecurity research and the desire to protect continued use and access to the technical components of those systems. Those research areas remain ripe for study, as demonstrated in the paucity of cross-domain collaboration of authors in their respective areas of expertise and discussed in the [Literature Review](#) chapter and specifically in the [Related Areas of Research](#) section.

Agent based models and cyber security research

Cyber-security research, especially when constrained to technology-focused models and questions of interest have ventured into the ABM realm less frequently than many other fields of research. This is certainly understandable when viewing computer network traffic as continuous flows of data packets, where individual packets, and even individual components of the network have little to no ability to perceive their environment and react to it. It is this broad view that is a common theme in the network emulators in (Lochin et al., 2012) review. Even in the pursuit of 'intelligent' networks and machine adaptation to network or component level challenges (e.g., component outage, rate control services (Gligor, 2005), load-balancing redirection (Pai et al., 1998; Wang et al., 2002)), the agents are not human agents, nor are the researchers usually making the leap to incorporate the sociological component of sociotechnical systems in the section title. In one NSA-sponsored cybersecurity forum, the organizers went so far as to constrain discussions by omitting 'humans' because 'they are hard to understand' and it is much less contentious to work on the technology side of research questions.

There have absolutely been efforts at evaluating the human-impacts of disruptions to or loss of the technical infrastructure. The research gap remains however between those efforts and the continuity of operations COI, the HRO COI and other efforts to understand the world we live in, especially when the world changes quickly or dramatically. Some efforts have incorporated human-enabled process modification (e.g., employing off-line backup capacity) (Pflanz, 2012; Pflanz & Levis, 2012) as a way of assessing the sustainability of time-sensitive missions in cyber-degraded environments. Others, such as RINSE (Leblanc et al., 2011) support Live and Constructive integration of human role players and simulations of technology as does the Department of Defense's Bulwark Defender exercise (Wihl et al., 2010). Multimodel modeling is also an approach to incorporating ABM M&S with technology focused M&S (Bigrigg et al., 2009; Kathleen M. Carley, Geoffrey P. Morgan, et al., 2012; Kathleen M. Carley et al., 2012; Elder & Levis, 2010). The cited examples have demonstrated modeling working in tandem though not interoperating. The methods would seem to offer fertile opportunities for researchers to use models with varying processing and generative internals. When outputs are congruent, researchers can reasonably argue higher confidence in the feasibility of the results.

This section has been a short refresher of the material discussed in [Literature Review](#) chapter. The intent has been to remind the reader that there are many related fields of research that a casual observer could reasonably infer share interests and information. The potential for such sharing of theories, methods, results, and understanding certainly exists, and this dissertation is but one example of a way to link related-yet-disparate research: technology enabled and dependent organizations' resilience to contested cyber environments.

Overview of Construct

Construct is an ABM developed over time at Carnegie Mellon University under the guidance and supervision of Dr. Carley. It has its roots in constructualism (Kathleen M. Carley, 1986), the view that the inhabitants of socio-cultural environments continually construct and reconstruct their environment through individual cycles of action, adaptation, and motivation. It is network-centric not only in its roots but in its implementation, internal data structures are frequently matrix representations of those networks—a sight familiar to practitioners of social network and graph-theoretic sciences. Construct has had numerous technical reports written since its inception, and I refer the reader to its User's Guide (Kathleen M. Carley et al., 2014),

predecessor Technical Reports and CASOS for up-to-date information and changes from its documentation. This section will provide a brief over-view of Construct's origins and internal functioning.

Initial instances of Construct had basic interaction mechanisms that embodied three (3) empirically identified human interaction generalizations. The first is that knowledge acquisition occurs through interaction (Leon Festinger, 1950) as cited by (Schreiber, Singh, & Carley, 2004). The second is that humans tend to interact with those who are similar to them, often called homophily and described in (J. M. McPherson & Smith-Lovin, 1987) and revisited by those authors in (M. McPherson, Lovin, & Cook, 2001) among many others. The third interaction pattern is social relativity, first discussed by Festinger (1954) and (Merton, 1957, 1968) (as cited by (Schreiber et al., 2004)). These three (3) patterns had up to five (5) moderators available to a researcher to use in experiments: forgetting, proximity, transactive memory, referrals, and access (Schreiber et al., 2004).

The roots of Construct as an information diffusion simulation are evident in the first interaction pattern and the principal motivation of agents in the simulation—the drive to interact with other agents to exchange information. The moderators of that drive are the agents' perceptions of similarity to other agents (transactive memory (Argote, 2003; Ren & Argote, 2001) and homophily) as well as proximity and synchronous availability. Knowledge retained and propagated has, as moderators, the forgetting rate(s), as well as stochastic probabilities of mishearing a message from other agent(s) as well as misstating knowledge when sending it.

Subsequent and modern versions of Construct added binary task completion and energy tasks (Moon, 2008) to the simulation. Binary tasks are used in traditional methods of studying organizational accuracy. Participants in the task attempt to discern the number of ones (1) or zeros (0) in a binary string, and pass their estimations or answers to others. Knowledge bits, pools of binary values representing knowledge available to agents, have links to these tasks (in the form of a Task x Knowledge network). These networks support the intuitive property that possessing higher quantities of linked knowledge leads to higher probabilities of agents and groups of agents accurately performing these tasks. In the absence of knowledge, agents must still make assessments and do so using reported assessments of agents to whom they are connected. Energy tasks are abstracted nonspecific tasks that reflect the reality of human agents

not spending their entire existence only talking with other agents. When enabled, agents will spend some portion of their simulation

Belief diffusion, an extension of knowledge diffusion and tied to the social relativity work of Festinger and others is in current-day versions of Construct. Real numbers ranging $[-1, 1]$ represent each stylized belief per agent. In this range of values, -1 represents a maximal negative valence and 1 represents a maximal positive valence to the belief. Researchers may create modeled beliefs rooted in possession of knowledge that contributes to positive or negative valence as well as modeling beliefs not directly related to knowledge. Self-perception as well as omniscient knowledge of other agents' beliefs contribute to homophily assessments and increase the probability of interactions—at the expense of increased computational time.

The final aspect of Construct to briefly discuss is its recent incorporation of social groups and *generalized other* (Mead, 1925) as cited in (Joseph, Morgan, Martin, & Carley, 2013). Joseph et al. adjusted Construct away from agents retaining perceptions of every alter-ego to which the agent has connection. In its newest incarnation, Construct agents, when faced with having no personalized perception of an alter, and consequently no basis to judge homophily, create an error prone interpretation of the alter based on knowledge of the social groups the alter belongs to (Joseph et al., 2013). This social stereotyping is akin to not personally knowing a political candidate, but inferring the candidate has certain beliefs and knowledge based on the avowed political party of the candidate. If there is no information about the group(s) the person belongs to, then inferences occur based on a people-in-general concept, often referred to as the *generalized-other* (Mead, 1925).

Through creation of appropriate input files, what the Construct's User Guide (Kathleen M. Carley et al., 2014) calls *input decks*, researchers provide Construct definitions of experimental variables, lists of input nodes, and network definitions. Construct can stochastically generate the networks using parameters in the input deck, read data from ORA™ DynetML files, or draw from other empirical sources. Node identifiers can also be from empirical sources, or simple integers from $[0..n]$ with n =number of nodes. I refer the reader to the Construct User's Guide for a more complete discussion of the input deck contents and to [Appendix 6](#) (starting on page [6-1](#)) for the deck I used for the operational and strategic modeling.

Augmentation of D2M generated models

There are two models of organizations (organization being an aggregation of multiple heterogeneous cognitively limited agents) I use in the dissertation: strategic and operational. To use the D2M models created in previous chapters, each requires a level of augmentation. Revisiting the dissertation workflow from , we can see where we are in the process by looking at the colored ovals and box in .

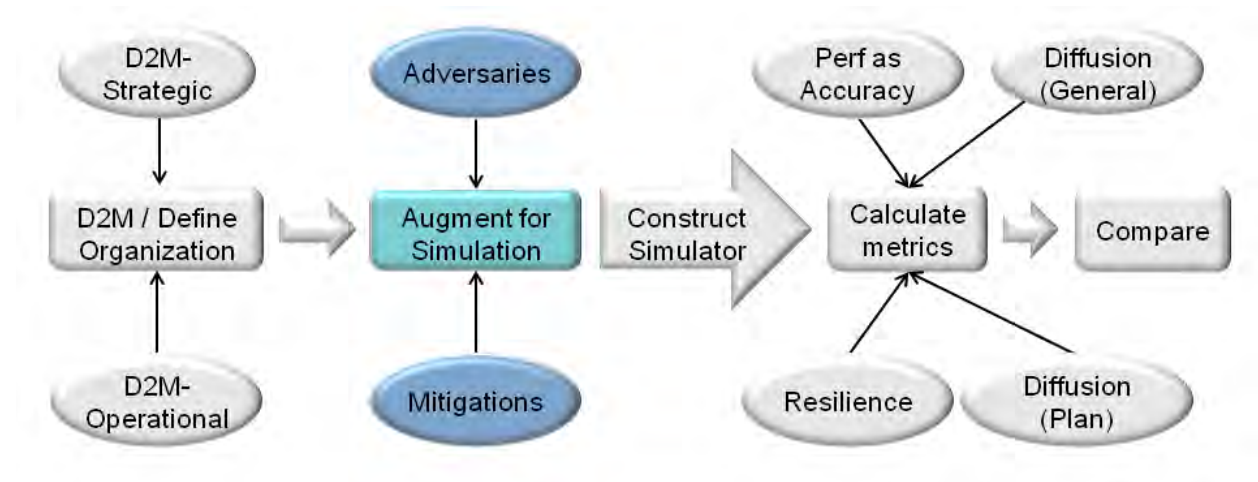


Figure 118: Dissertation workflow augmentation of models for use in ABM

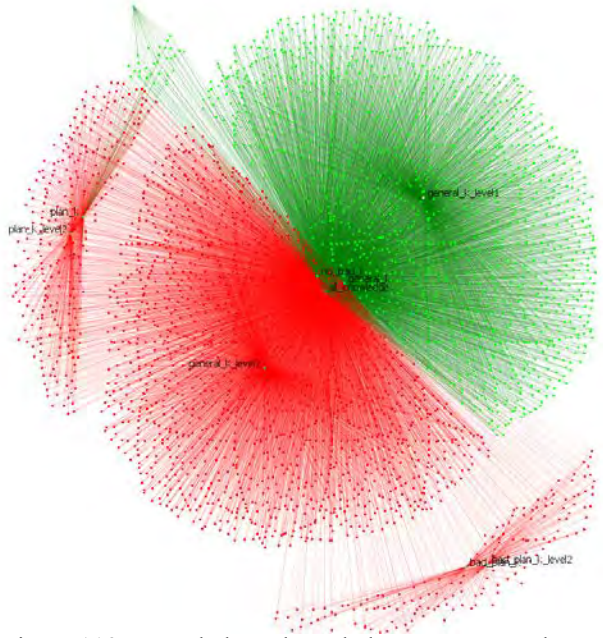
The source documents I used do not discuss many of the particular inputs Construct needs to function, though this shortfall is likely more manageable with use of proprietary or sensitive documents instead of public documents. Additionally, the initial modeling effort deliberately used the entire ontology for metanetwork node types. Not all the node types in the metanetwork ontology are useful to Construct which leads to both descopeing the metanetwork model as well as augmenting it for processing by Construct.

The table below is roster of changes and modifications to the metanetwork ontology. There are a total of thirty modifications needed on the D2M model for Construct to be able to make complete use of the model.

Table 51: Exogenous modifications to D2M models

Item #	Action	Of What	Why and Discussion
1.	Added nodes	agent nodeset	<p>Where I had no data to discern a classification level, I created a new instance of the agent or IT agent. I assigned this new instance the ‘level 2’ attribute and assigned ‘level 1’ to the D2M-identified agent or IT agent.</p> <p>In this manner, a geospatial_database IT agent would get a twin called geospatial_database_level2.</p>
2.	Added nodes	agent node set	<p>I manually create a confidentiality sink agent and assigned it a ‘level1’ attribute for each model.</p> <p>This agent is responsible, when active during confidentiality attacks, for receiving communications from other IT agents. Assessment of the organization is the tendency of level2 knowledge to flow to and within level1 agents—representing a classification leak though without specific operational impacts.</p> <p>Assignment of links to level1 key IT agents used the same random binary graph generator and equation (39)</p>
3.	Added nodes	agent node set	<p>I manually create an integrity agent for each level of each model.</p> <p>This agent is responsible, when active during integrity attacks, for disseminating bad information into the organization.</p>
4.	Added nodes	agent node set	<p>Roles do not exist in Construct. I recoded all roles as agents, though I retained an attribute on the imported roles listing them as ‘role’</p>
5.	Added nodes	agent node set	<p>I recoded all IT agents that the D2M process generated as construct agents. I did however retain an attribute that labels the recoded agents as ‘it_systems.’</p> <p>Construct supports different behaviors for different agent types, and the IT agents have a reduced probability of forgetting, higher quantities of communication reception counts than human agents. IT Agents have the same communications initiation counts as human agents, and with the disparity between initiate and receive, they are more akin to ‘pull’ IT systems than ‘push’ IT systems.</p>

Item #	Action	Of What	Why and Discussion
6.	Added nodes	knowledge node set	<p>Where I had no data to discern a classification level, I created a new instance of the knowledge node. I assigned this new instance the 'level 2' attribute and assigned 'level 1' to the D2M-identified knowledge node.</p> <p>This heuristic possibly over generalizes the amount of information in an organization but it decreases processing time for model generation. It also acknowledges that a knowledge concept may well reside with two (2) slightly different instantiations: unclassified and classified.</p>
7.	Added nodes	knowledge node set	<p>I manually created a set of knowledge equal to 10% of the knowledge set to represent a 'plan.'</p> <p>10% of plan knowledge received a 'level 1' attribute 90% of plan knowledge received a 'level 2' attribute</p>
8.	Added nodes	knowledge node set	<p>I manually created 'bad plan' knowledge at ratio of 10:1 (good:bad) for level 1 and level 2.</p> <p>I manually assigned these two sets of knowledge to their respective knowledgegroup.</p> <p>I manually assigned integrity agent level 1 to bad plan knowledge level 1.</p> <p>I manually assigned integrity agent level 2 to bad plan knowledge level 2.</p>
9.	Added nodes	knowledgegroup node set	<p>I manually segregated the D2M generated knowledge pool into five (5) major groups, and eleven total sub-groups. The dissertation is asking questions about the resilience of planning organizations in the face of contested cyber environments. But having only 'information of interest' in the simulation is a degenerate design case and uninteresting from a research perspective.</p> <ol style="list-style-type: none"> 1. All_knowledge 2. General_knowledge <ol style="list-style-type: none"> 2.1. General_knowledge_level1 (all level 1 non-plan knowledge) 2.2. General_knowledge_level2 (all level 2 non-plan knowledge) 3. Plan_k <ol style="list-style-type: none"> 3.1. Plan_knowledge_level1 (see next row for details) 3.2. Plan_knowledge_level2 (see next row for details) 4. Bad_Plan_K <ol style="list-style-type: none"> 4.1. Bad_plan_knowledge_level1 4.2. Bad_plan_knowledge_level2 5. No Bad K (General_K + Plan_K)

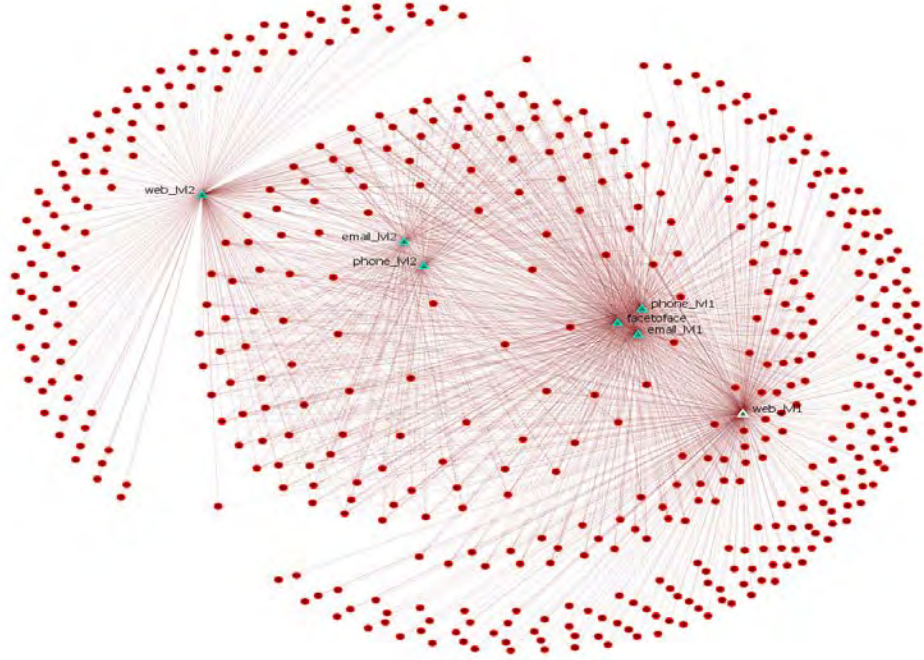
Item #	Action	Of What	Why and Discussion
			<p>operational ORA file with spares</p>  <p>Figure 119: Knowledge x knowledgegroup network</p>
10.	Added nodes	Location node set	<p>I added nodes for the headquarters of all the commands of interest. For those commands where I did not have an exact location I used Google Maps and a general search to provide a latitude and longitude (e.g., Al Udeid Air Force Base, Doha, Qatar)</p> <p>I also added an 'other' node for those organizations for which I had no evidence of an actual location. This was particularly true for IT systems. For the geographical location of this other, I chose Fort Knox, Kentucky as it was somewhat near the geographical center between Washington DC and Barksdale AFB for the Strategic Model. For simplicity I left it the same for the Operational model as well.</p>

Item #	Action	Of What	Why and Discussion	
11.	Added nodes	organization node set (aka agentgroup)	<p>I added a JPG group and ‘JPG Briefing’ groups to each model’s organization nodeset.</p> <p>The dissertation is asking questions about the resilience of planning organizations in the face of contested cyber environments. Focusing on the planning nature of these organizations, allows me to have a set of agents (the JPG) that receives a ‘plan’ from some exogenous source.</p> <p>A method of assessing organizational resilience is to trace the flow of plan information from this JPG to the remainder of the agent population. More specifically, the dissertation attempts to identify differences in uncontested environments and contested environments in the speed and accuracy of information flow to the various sets of decision makers (the attendees of the JPG Briefings) in the models.</p>	
12.	Deleted nodes	Belief node set	<p>Incorporation of beliefs was beyond the scope of this effort. I deleted the entire belief node set.</p> <p>Future work could easily generate questions of interest and incorporate beliefs into future models.</p>	
13.	Deleted nodes	Event node set	<p>The only specific event modeled in the scenarios under test was the plan-brief-plan cycle.</p> <p>Construct could not draw this cycle from the list of events the D2M process generated, so Construct does not use these nodes or networks.</p>	
14.	Deleted nodes	IT Resources (aka Communications Mediums)	<p>I deleted all the IT resource nodes in the D2M generated models and kept seven (7) nodes per model. These nodes are what Construct calls ‘Communications Mediums.’</p> <p>For any two agents to interact, not only must they have a connection in the agent x agent network, they must both have access to a common communication medium.</p>	
			Operational	Strategic
			<ol style="list-style-type: none"> 1. Unclassified Telephone/Voice 2. Classified Telephone/Voice 3. Unclassified IP networks 4. Classified IP networks 5. Face-to-Face (f2f) 6. Unclassified Email 7. Classified Email 	<ol style="list-style-type: none"> 1. Unclassified Telephone/Voice 2. Classified Telephone/Voice 3. Unclassified IP networks 4. Classified IP networks 5. Face-to-Face (f2f) 6. Unclassified Email 7. Classified Email

Item #	Action	Of What	Why and Discussion	
15.	Deleted nodes	organization node set (aka agentgroup)	<p>I down selected organizations, <i>manually</i>, in the D2M models to a set of suborganizations of interest as noted below for each of the two models.</p> <p>I manually deleted organizations with less than 3 x D2M-discerned edges in them—with the exception of the manually added groups (e.g., confidentiality agent group, and integrity agent group) and groups necessary to maintain organizational face validity.</p> <p>I added groups for assessing collections of agents that the D2M process did not otherwise capture. See also the entry for adding nodes to the organization node set.</p>	
			Operational	Strategic
			COCOM Staff (J1...J9) AFSCC/NAF Staff (A1..A9) JCOAC Divisions (x5) Wing and Below USAF/Service Cyber JPG	NCA related NSC & NSC Staff CJS & JS (J1..J9) USSTRATCOM USSTRATCOM JPG USCYBERCOM Intelligence Community (IC) Military Departments (MILDEP) Other Gov't Agencies (OGA) Geographic Combatant Commands (GCC) Functional Combatant Command (FCC)
16.	Deleted nodes	Location node set	I deleted all nodes that did not have a geographically identifiable location (e.g., Barksdale Air Force Base).	
17.	Deleted nodes	Resource node set	Resources do not exist in Construct with its origins in belief and information diffusion. I deleted the entire resource node set the D2M process generated.	
18.	Added node attributes	agent nodeset	<p>The corpus rarely discussions clearance requirements for roles and individuals. For each human and IT agent, I assigned them a node attribute of 'human' or 'it_system.'</p> <p>The corpus rarely identified IT systems as 'IT systems' and usually simply referred to generic IT systems or named and specific systems. I therefore manually reviewed each of the retained agents to identify if they were 'human' or 'IT.'</p>	

Item #	Action	Of What	Why and Discussion
19.	Added node attributes	agent nodeset	I added an attribute to each node entitled 'key' and treated it as a Boolean. I marked those agents from the Key Entities chapter as 'key' and used that as an exogenous marker for differentiating key IT agents
20.	Added node attributes	knowledge nodeset	<p>Differentiation of sensitive and nonsensitive knowledge The D2M corpus rarely directly differentiates which knowledge concepts belong to which levels of classification domains. To remediate this shortfall, and assist in the rapid modeling process I used the following heuristics and methods to segregate the single knowledge node set into two nodesets.</p> <ul style="list-style-type: none"> • Knowledge nodes connected only to IT systems (Level 1) stayed in level 1 knowledge • Knowledge nodes connected only to IT systems (Level 2) stayed in level 2 knowledge • Logistics, Medical, and Personnel 'intel, ' and 'plan' nodes stayed with level 1, while military operations centric intel nodes stayed with level 2 • All publications stayed with level 1 knowledge •
21.	Added edges	agent x agent network agent x organization network organization x organization network	<p>Most organizational models, to at least establish face validity, need to reflect lines of authority. The D2M process did not always capture the chains of command a reader would expect of military organizations. The D2M corpus frequently did not adequately reflect the details of the command hierarchies for both levels of warfare.</p> <p>As such, a <i>manual process of edge creation</i> in the agent x agent, organization x organization, and agent x organization networks based on SME input and my own professional expertise was necessary to augment the automation-based models with additional relationship edges between organization nodes.</p>
22.	Added edges	agent x agent	When I duplicated agent nodes to create 'level2' agents, I needed to duplicate the edges each 'level 1' twin had, but inside the 'level2' agent set.

Item #	Action	Of What	Why and Discussion
23.	Added edges	agent x agent	<p>When I created integrity agents, I needed to have them connect to other agents to enable dissemination of their information. I chose to target the Key IT systems as the targeted systems, based on the static assessments of large effects created by targeting small but important quantities of IT systems.</p> <p>I used a random binary graph generator within Construct with a mean value set with the equation shown below. In other words, if the probability of an integrity attack was 0.8, the integrity agent would have a probability of 0.8 for receiving an artificially created link between it and any particular key IT agent.</p> $P_{\text{interaction}} = \begin{cases} 1, & \text{random} < \text{Probability}_{\text{integrity attack}} \\ \text{else } 0 \end{cases} \quad (39)$ <p>Equation 39 agent x agent probability of interaction</p>
24.	Added edges	Agent x communications medium network	<p>I manually created links between agents and communications media using the following heuristics:</p> <ul style="list-style-type: none"> - Human (level 1 and level 2) to human (level 1 and level 2): f2f, level1 phone - Level 2 Human to Level 2 Human: level 2 phone, level 2 email - Level1 Human to Level 1 IT Agent: level 1 IP network - Level 2 Human to Level1 IT Agent: level 1 IP network - Level 2 Human to Level 2 IT Agent: level 2 IP network - Level 1 IT Agent to Level 1 IT Agent: level 1 IP network - Level 2 IT Agent to Level 2 IT Agent: level 2 IP network

Item #	Action	Of What	Why and Discussion
			 <p>Figure 120: Agent x Communications Medium (Operational)</p>
25.	Added edges	agent x organization network organization x organization network	<p>Organizations (aggregations of humans for common purposes/tasks) do not exist as explicitly modeled entities in Construct. Instead, modelers can exogenously assign agents to groupings of Agents that help fulfill the stereotyping of perceived similarity capability. Such grouping also supports output analysis at various levels of aggregation.</p> <p>The Agent x Organization links derived from the D2M process are far too sparse to support the Construct group membership stereotyping.</p> <p>I added ed edges between agents and organizations that I knew existed based on my military experiences. I also added edges based on samplings of the corpus.</p>

Item #	Action	Of What	Why and Discussion
26.	Added edges	agent x organization organization x organization	<p>After I manually created the JPG and JPG Briefing Group for each model I created links between elements habitually included in JPGs (e.g., intel, ops, ops planners, logistics planners, staff judge advocate, targeters).</p> <p>The D2M models may have words that semantically mean JPG briefing, but there is no other sense of a time-driven event in the D2M models. Instead the plan-brief-plan cycle is implemented using the following heuristics within the simulation</p> <ul style="list-style-type: none"> - 1/3 of the time period after the simulation warm-up is set aside for ‘planning.’ This corresponds to a military heuristic of 1/3:2/3 time division between the planning organization and the implementing organization. - A starting value of 20% of the ‘planning’ time is set aside for ‘briefings’ - The JPG is incentivized to interact with each other by more heavily weighting expertise seeking behavior during the plan-brief-plan cycle. - There is a large group of
27.	Added edges	Organization x location	I manually created links between the organizations of interest and the locations of interest.
28.	Deleted edges	Agent x knowledge network	I manually removed links between level 1 Human and IT agents and level 2 knowledge. I allowed level 2 agents and systems to remain connected to level 1 knowledge.
29.	Edge modification	agent x agent network	<p>I binarized the agent x agent interaction network the D2M process generated. Edge weights were co-occurrence counts in the source documents, and otherwise not of benefit to the simulation process.</p> <p>Co-occurrence counts for the IT systems, especially after sampling and reading source documents indicate a common interpretation: there is some logical inter-dependency of the systems. An example of this would be a web server linked to a database is representing a logical dependency with the actual physical or network-level interconnection abstracted away from the model.</p>
30.		Warm Up Period	<p>As noted in Figure 2 and Figure 85, I use a warm up period to establish an equilibrium point in the organization prior to executing attacks.</p> <p>I used a mathematical model that incorporates agent forgetting lead and the volume of data communicated at each interaction to estimated equilibrium points for both strategic and operational models.</p>
31.	Added network	Physical proximity network	Construct supports inferring a distance measure thorough the use of geodesic distances and edge weights, but I decided to use geographical distances, scaled and inverted as

Item #	Action	Of What	Why and Discussion
			Construct expects—a distance of 1.0 indicates two agents are maximally close, while a distance of 0.0 indicates the agents are maximally distant.
32.	No Change	Task node set	<p>I did not differentiate sensitive and non-sensitive tasks.</p> <p>The implication is that such tasks can require level 1 and level 2 personnel and knowledge.</p>

Adversary definition and setup for contested cyber environments

Instead of developing an adversary with a defined set of capabilities and motivations, this dissertation moves directly to predicted and simulated effects of an adversary's actions. In this effort, adversaries have, implicitly, finite capabilities and implicit motivations. The scenarios put under test here demonstrate an approach well beyond negligible threat, but equally well short of omniscient threat. I do make overt assumptions about adversarial capabilities, but in a direction orthogonal to the warnings of adversarial assumptions and resulting bad policy (Gligor, 2008).

Each of the three effects under test in the next chapter, loss of confidentiality, loss of integrity, and loss of availability are mid-term effects of a cyber attack. The loss, from near zero to total, of any of these three pillars of information assurance and security, are in themselves, rarely the sought-after effect in contested cyber environments. Rather, they are a component in efforts to deny friendly forces synchronized command and control of resources, with the subsequent effect of creating opportunities (e.g., military advantage, commercial advantage, possession of intellectual property, embarrassment, criminal opportunities) for an adversary to exploit. By inserting attack agents into each model at each classification level to act as a source for 'bad' knowledge to diffuse within the organization, I am implicitly granting my nameless adversaries the capability to conduct actions akin to advanced persistent threats (APT). The adversary has at his/her disposal, in each of the integrity attack conditions, the ability to inject bad data into the friendly organizations. Previous work (Lanham, Morgan, & Carley, 2012) has already demonstrated that with no screening criteria for clearly 'bad' knowledge, an adversary can have bad information diffuse throughout an organization. The same work also demonstrated that the bad knowledge, even if given an extremely short time-to-live, is incredibly long-lived: in general up to an order of magnitude longer than the original injection time!

In the loss of availability scenarios, I again choose to not posit a particular scenario that lead to the loss of key IT system availability—I simply assert there are instantaneous losses of availability at specified times. I grant the adversary (e.g., a malicious person, persons, nation-state, natural weather event) the ability to temporarily render one or more agents inaccessible while making the motivations of the contested cyber environment opaque. In this way, I'm attempting to avoid the numerous arguments and point/counter-point debates about plausibility and instead move to the more important aspect, for this dissertation, of assessing post event

resilience. I do not dispute the arguments by Cohen (F. Cohen, 1999) and Leblanc (F. Cohen, 1999; Leblanc et al., 2011) that adversary models should include capabilities and resource. Nor do I dispute that when research questions involve adversary motivations that scenarios and experiments should address such as advocated by (Gligor, 2008; Parker et al., 2004). The absence of these pieces of adversarial information is indicative that the information is not essential to the study of resilience to posited adversary-caused effects.

Finally, for the loss of confidentiality effect, I have chosen to model an adversary who is not pursuing an aggressive penetration and exploitation style of cyber attack. The technique I have chosen is to mimic a passive device targeted at ‘key IT systems’ and whose purpose is to collect data. It is an imperfect data capturing device, and is active at only specified time periods. This is a very general form of a confidentiality threat, much less than a key logger, and yet more than a data sniffer on a random piece of hardware. I do not attempt to assert a particular motivation for the confidentiality agent, nor do I have a particular end state for what some remote adversary would do with the captured data.

IT capabilities for D2M organizational models

Underlying telecommunications and networking infrastructure systems (e.g., [TELCO POPs](#), signal regeneration points) are abstractions contained but not otherwise addressed in the Construct simulation’s implementation of communications mediums. As noted in [Table 51](#), both D2M generated models have communications mediums of face-to-face, email, phone, and IP-based networks (the only way for IT agents to interact with other agents of any variety). Each of these mediums exist at each of the security levels. This gives a total of seven (7) communications mediums per model.

Classification levels for D2M organizational models

Organizations, civilian and military, frequently handle information and communications at several levels of sensitivity. In the military, these are typically the classification levels of unclassified (with and without handling caveats such as *For Official Use Only*), secret (with and without compartmentalization indicators), and top secret (with and without compartmentalization indicators). Civilian organizations may or may not use these same levels, but this proposal makes the simplifying assumption that both organizations operate with two levels of sensitivity: level 1 and level 2.

As described in [Table 51](#), the corpus of documents for each organization rarely makes explicit reference to the classification levels of the personnel or the IT systems those personnel have access to. With [SME](#) input and personal experience as well as on-line research, I differentiated the corpus-named IT systems by putting the correct classification domains on those systems. The agents (IT and Human) with the level 2 attribute set, have direct access to both levels of knowledge. Level 2 humans have access to both levels of IT systems, while level 2 systems will only be able to connect to other level 2 systems. Inter-connecting level 1 and level 2 systems does not happen in this dissertation, though future work could include such interconnections. The DoD calls such interconnections across classification domains cross domain solutions ([CDS](#)).

IT systems' capabilities and limitations for D2M organizational models

In each type of model, IT systems are agents with different sets of limitations and capabilities than human agents. IT systems are, themselves, agents within the simulation, but they are able to communicate with more agents per turn in both send and receive mode. IT systems communicate more complex messages per turn than do human agents. IT Systems do not lie, and they rarely forget facts compared to human agents. IT systems do not have beliefs, and they can suffer from availability attacks where, even if present in the simulation, they are unable to communicate with other agents in the simulation until the attack is over.

Shared planning, or operations order (OPORD), knowledge for D2M models

There is also, as part of the scenarios in use by the dissertation, a shared common set of 'planning' knowledge. These knowledge bits, shown below in [Figure 121](#) as blue dots, have multiple links with red agents. The six (6) red agents in this particular figure are 'Key IT' systems in the classified and unclassified domains. These systems connect to the knowledge as well as provide interorganizational links to their peer systems in other organizations. The blue dots in the upper right corner of [Figure 121](#) represent the starting configuration of a test run where only the singular Level 2 IT system per organization had access to all the plan data.

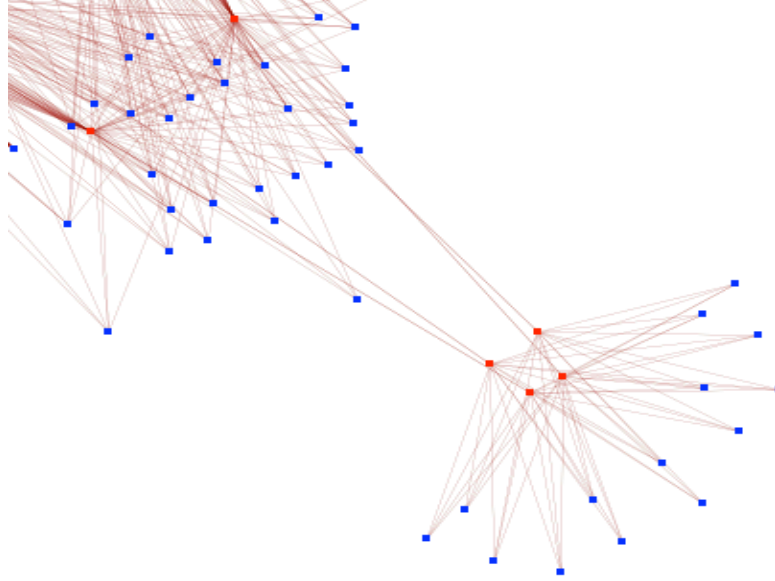


Figure 121: Shared planning knowledge

Inferring physical proximity for agents

Physical proximity, as well as the perceived difficulty of overcoming such distance (Conrath, 1973), is a well known mediator to communications. Construct uses physical proximity in its calculations of interaction probabilities on an agent x agent basis every turn. To support this use, Construct needed data. To generate data, especially in the near complete absence of geographical locations and distances in doctrine, it is necessary to apply additional data generating techniques. There were twelve steps to the process of calculating a physical proximity network.

Location by Location network with links as distance in kilometers

After down selecting nodes in the location node set, I created nodes for the approximate locations of each of the organizations and commands of interest. Google maps™ offered a fabulous opportunity to generate geospatial data independent of classified data sources. By adding latitude and longitude to each location, I was then able to export the data to Excel and calculate the pair-wise distance between all locations. I used the law of cosines to calculate the distances in kilometers using the equation below, and $\varphi_1 = \text{latitude}_{\text{location A}}$, $\varphi_2 = \text{latitude}_{\text{location B}}$, and $\Delta\lambda = \text{longitude}_{\text{location B}} - \text{longitude}_{\text{location A}}$ all in radians.

$$d = \cos^{-1}(\sin \varphi_1 \times \sin \varphi_2 + \cos \varphi_1 \times \cos \varphi_2 \times \cos(\Delta\lambda)) \quad (40)$$

Equation 40: Law of Cosines to calculate distances between two points on a sphere

Creating a Agent x Location network, count of common organizations

The next step was to create a network of Agents by organizations where the link values are the counts of shared organizations. This will give me a denominator for calculating the average distance across all same-agents at multiple organizations—in other words an agent George may be common to multiple organizations and this will generate the count of those shared organizations Using previously discussed node set and matrix notations, the equation to generate this network is shown below.

$$\mathbf{AL} = \mathbf{AO} \times \mathbf{OL} \quad (41)$$

Equation 41: Generating an agent x location network (count of shared organization)

Creating a Agent x Location network, sum of distances between egos

The next step was to create a network of Agents by locations where the link values are the sums of distances across all the instances of each particular agent at each location.

$$\mathbf{AL} = \mathbf{AL}_{dichotomized} \times \mathbf{LL} \quad (42)$$

Equation 42: Generating an agent x location network (sum of distances between ego instances)

Creating a Agent x Agent network, count of common locations

The next step was to create a network of Agents by agents where the link values are the counts of shared locations.

$$\mathbf{AA} = \mathbf{AL} \times \mathbf{AL}^T \quad (43)$$

Equation 43: Generating an agent x agent network (count of shared locations)

Creating a Agent x Agent network, sum of distances between egos and alters

The next step was to create a network of Agents by agents where the link values are the sum of distances between each ego (row agents) and their alters (column agents). I use [\(42\)](#) to assist in calculating this value and show the equation below.

$$\mathbf{AA} = \mathbf{AL}_{43} \times \mathbf{AL}^T \quad (44)$$

Equation 44: Generating an agent x agent (sum of distances between egos and alters)

Cell-wise division to generate average distance between egos and alters

The next step is to generate the average distance, by dividing each cell of (44) by the sum of the respective cell in (43) and the row sum of the ego in the agent x location network. This is more easily depicted in the equation below.

$$\mathbb{A}_i \mathbb{A}_j^{\text{physical proximity}} = \frac{\mathbb{A}_i \mathbb{A}_j^{\text{sum of ego-to-alter distances}}}{\mathbb{A}_i \mathbb{A}_j^{\text{shared loc count}} + \mathbb{A}_i \mathbb{I}_j^{\text{row count}}} \quad (45)$$

Equation 45: Generating average distance between ego and alter agents

Cell-wise inversion and return to ORA™ the agent x agent physical proximity network

The last step in generating the physical proximity network, where the links represent the average distance between egos and alters, is to cell-wise invert the values to achieve the scale Construct expects of [1.0,0], for maximally close and maximally distant.

$$\mathbb{A}_i \mathbb{A}_j = \begin{cases} 1, & \text{if } i = j \\ \frac{1}{\mathbb{A}_i \mathbb{A}_j}, & \text{otherwise} \end{cases} \quad (46)$$

Equation 46: Generating an agent x agent physical proximity network for use by Construct, scale [1.0,0.0]

With the copying of the results of (46) back into ORA as a network called ‘physical proximity’ the modeler has provided Construct with the data to computer the physical proximity component of interaction probabilities between agents.

Experimental Design Setup

As previously discussed, there are two text mined models. For each model, I put under test various combinations of cyber effects (i.e., confidentiality, integrity, availability) targeting specific IT systems or more general communications mediums. A graphical representation of the DMU’s in these models and their connections to the systems under attack is shown in [Figure 122](#). The intent of the experiments was to judge if the graphical representations of resilience of measures of interest (MoI) (see [Figure 2](#) and [Figure 85](#)) were theories with empirical foundations and to what degree. Additionally, the expectations of the experiment were to fulfill another deliverable of the dissertation, a rapid multi-dimensional assessment of resilience of organizational models that were themselves rapid constructions from self-documentation. Finally,

two broad categories of mitigations were put under test: functional changes and organization structure changes, operationalize as new arrival training, spare/replicas of Key IT systems and procedures for bringing them on-line, and changing the ratio of meetings to planning sessions.

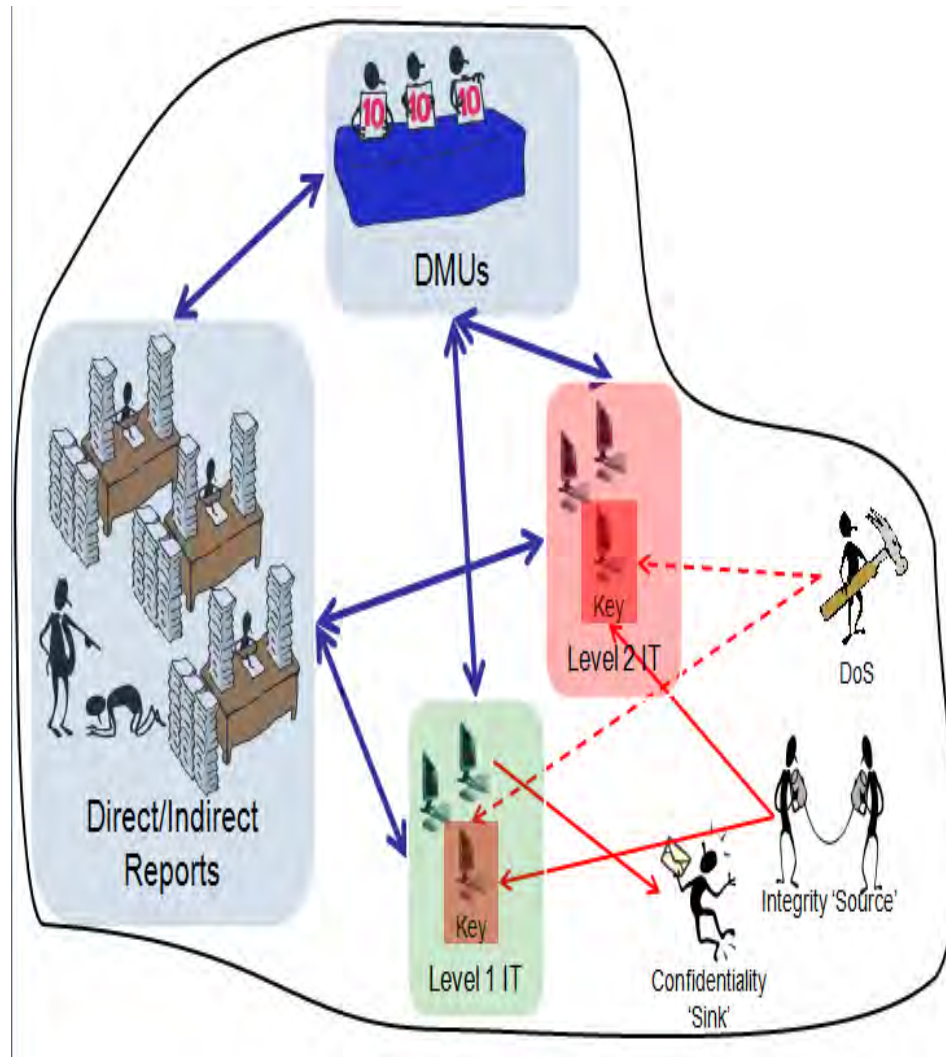


Figure 122 Graphical representation of organization under test

New arrival training informs new members of the organization who-knows-what and who-does-what. These correspond exactly with Construct's ability to implement knowledge transactive memory and task assignment transactive memory. New arrival training has a history of improving organizational performance (Bartel, 1994) with Tracey et al building the General Training Climate Scale to provide feedback to management (Tracey & Tews, 2005). Within the military, this is akin to a new arrival receiving an overview briefing of the organization with fairly explicit details about what each staff section and sub-section does, as well as learning the names of members in those sections. Learning what the sections do (task assignments) supports

individual agents in creating generalized perceptions of all agents in the subsections. By varying the false positive rates and false negative rates for each of the types of perceptions, I expect the modeled organizations to have better performance with low false rates for all four variables.

The second change, use of replica Key IT systems (and their starting knowledge) and varying how fast the equipment is brought online, increases knowledge redundancy within the organization. Redundancy as a means of improving resilience to disruptions is a known technique in multiple fields: public-key cryptosystems (Frankel, Gemmell, Mackenzie, & Yung, 1997), design of control systems in critical infrastructures (Rieger, Gertman, & McQueen, 2009), provision of public services (Low, Ostrom, Simon, & Wilson, 2003), and is frequently seen in functional redundancies in ecosystems (Low et al., 2003). The US Chemical Safety and Hazard Investigation Board (Crichton et al., 2009) specifically calls out widespread distribution of knowledge, especially of past organizational failures. The variable aspect of this component is how fast mitigation techniques are fully in effect—analogous to rehearsals that improve the ability of organizations to react to situations.

The last mitigation I experiment with is the varying of the meeting to planning ratio for the [JPG](#) and JPG briefing attendees. In time compressed environments, the military already practices something like this mitigation—it is sometimes called an abbreviated military decision making process. Abbreviated [MDMPs](#) usually require more participation by leaders (more ‘meetings’ or larger audiences) and less time by specialized planners (JPG planning) isolated in their planning cell. Changing meeting time ratios and attendees are both techniques common in the emergency management services (Comfort, 2006). I expected modeled organizations with this mitigation to have better performance than the baseline up to a point, and then I expect a worsening return on investment of leaders’ time.

The verbiage of the variables placed under test can get daunting. In addition to the explanations above, I offer two additional aids: a graphical rendering of the factorial tree of categorical variables with Box-Behnken leaves, and a set of tables.

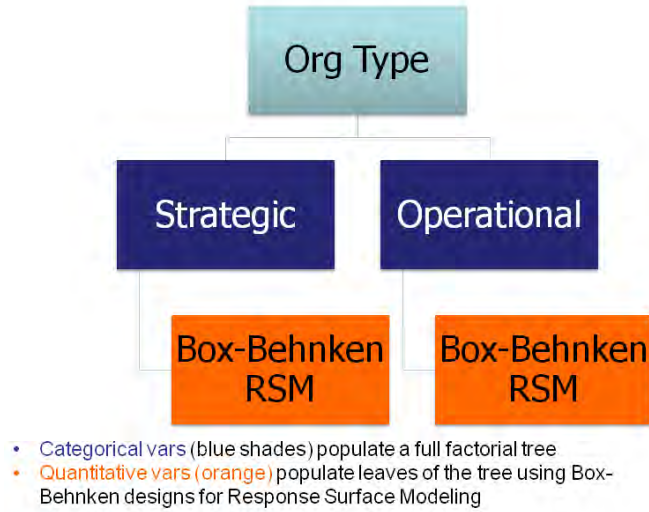


Figure 123: Graphical rendering of experimental setup with factor tree and Box-Behnken leaves

Table 52: Experimental summary for D2M generated models

Condition	Possible Values	Quant. Combos	Cat. Combos
Organizational Model	Strategic, Operational		2
Confidentiality Attack <i>IT</i>	$P_{\text{effect}} = 0.0, 0.2, 0.8$	3	
Integrity Attack <i>IT</i>	$P_{\text{effect}} = 0.0, 0.2, 0.8$	3	
Availability Attack <i>IT</i>	$P_{\text{effect}} = 0.0, 0.2, 0.8$	3	
Availability Attack (email)	$P_{\text{effect}} = 0.0, 0.2, 0.8$	3	
Availability Attack (phone)	$P_{\text{effect}} = 0.0, 0.2, 0.8$	3	
Availability Attack (web)	$P_{\text{effect}} = 0.0, 0.2, 0.8$	3	

Mitigations:			
Knowledge tm false positive rate	$P_{\text{effect}} = 0.05, 0.1, 0.2$	3	
Knowledge tm false negative rate	$P_{\text{effect}} = 0.05, 0.1, 0.2$	3	
Task tm false positive rate	$P_{\text{effect}} = 0.05, 0.1, 0.2$	3	
Task tm false positive rate	$P_{\text{effect}} = 0.05, 0.1, 0.2$	3	
Speed of Mitigation in Plan-Brief Cycles	0,1,3	3	
Meeting-Plan Ratio	0.20, 0.40, 0.60	3	

A naïve implementation of the experimental table above would yield a factorial result shown below. Clearly this is an infeasible number of iterations especially given runs times of 1 - 5 minutes per turn, even across a high throughput computing cluster.

$$2 \text{ models} \times \frac{3^{11} \text{ combinations}}{\text{model}} \times \frac{20 \text{ iterations}}{\text{combination}} = 7,085,880 \text{ iterations} \quad (47)$$

Equation 47: Naive experimental design and summary

Instead of planning on a naïve implementation as shown in (47), I turned to the Box-Behnken designs for response surface modeling (RSM) (Box & Behnken, 1960). The 10 factor design, called ‘Design 7’ in the above looks like the table below, where ± 1 indicates to the modeler to take the top and bottom values of the three specified values for that variable.

Table 53: 10 factor Box-Behnken design

Factor 1	Factor 2	Factor 3	Factor 4	Factor 5	Factor 6	Factor 7	Factor 8	Factor 9	Factor 10
0	± 1	0	0	0	± 1	± 1	0	0	± 1
± 1	± 1	0	0	± 1	0	0	0	0	± 1
0	± 1	± 1	0	0	0	± 1	± 1	0	0
0	± 1	0	± 1	0	± 1	0	0	± 1	0
± 1	0	0	0	0	0	0	± 1	± 1	± 1
0	0	± 1	± 1	± 1	0	0	0	0	± 1
± 1	0	0	± 1	0	0	± 1	± 1	0	0
0	0	± 1	0	± 1	0	± 1	0	± 1	0
± 1	0	± 1	0	0	± 1	0	0	± 1	0
0	0	0	± 1	± 1	± 1	0	± 1	0	0
0	0	0	0	0	0	0	0	0	0

Expanding [Table 53](#) and including ten (10) iterations of the last combination (the baseline condition), this RSM technique allows me to reduce the number of iteration substantially. The final number of combinations per model is 179, yielding the equation below for the number of iterations within the experimental design.

$$2 \text{ models} \times \frac{179 \text{ combinations}}{\text{model}} \times \frac{20 \text{ iterations}}{\text{combination}} = 71,600 \text{ iterations} \quad (48)$$

Equation 48: Box-Behnken experimental design and summary

The expanded and colored version of this spreadsheet is also [Table 53](#) on page 195. The colorized versoin (red=low, yellow=mid-value, green=high value) helps depict the design. A 2D projection of the sum of the attack and mitigation value, [Figure 124](#). I added 13 conditions into the plan to reduce the probability of missing critical zones and interaction. The large black line after the sixth column divides the table between probabilities of attack effect and the mitigations. Though there are six columns for mitigations, the knowledge transactive memory false positive rate and task transactive memory false positive rate columns vary at the same time. The false negative rate columns are equally tied to to each other. This, in effect, changes the six column representation to four mitigations in practice.

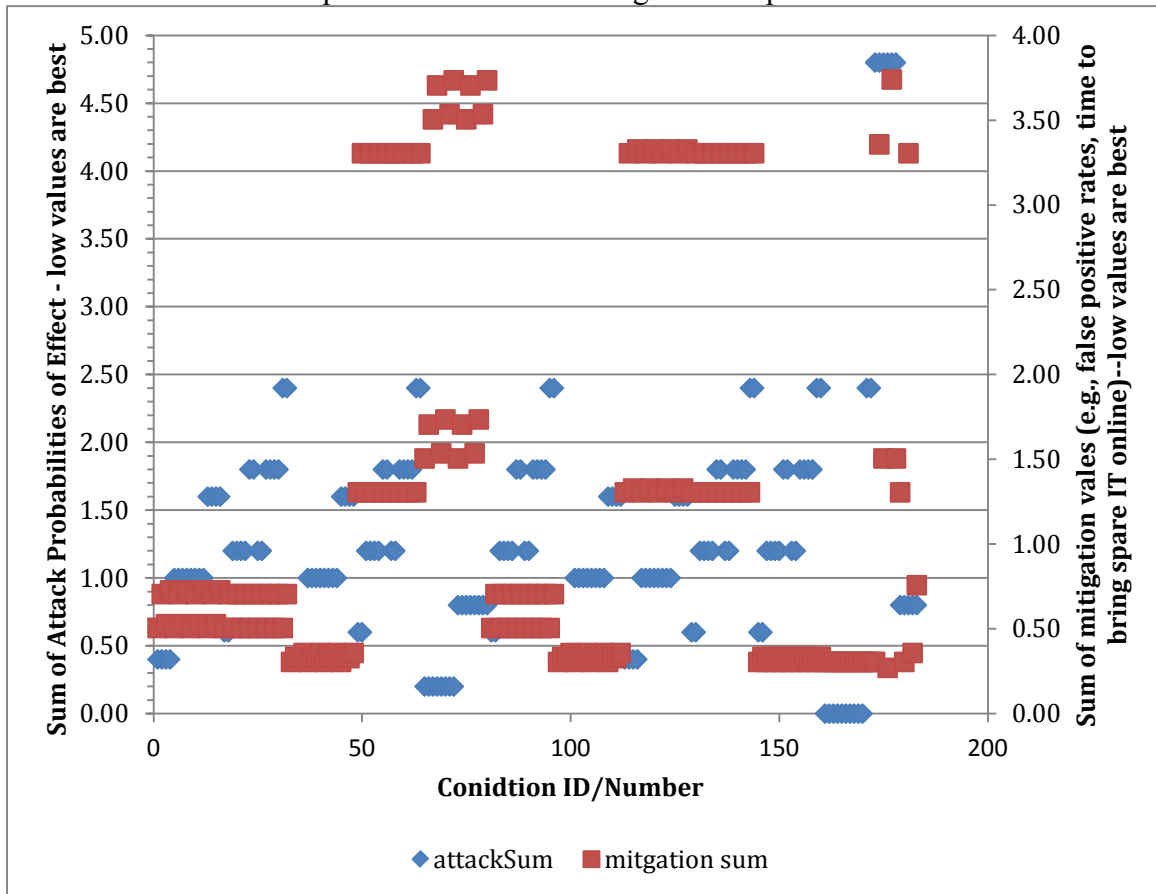


Figure 124: Visual representation of distribution of sums of attack probabilities and mitigations' values

Conclusion

In the abstract and Introduction chapter, I discuss four demands leaders should place on their organization to increase their assurance of resilience to contested cyber environments. This chapter has contributed to the second, third, and fourth of those demands. With the processes and methods in this chapter, organizational leaders can more rapidly model their organizations, their organizational vulnerabilities, and prepare the model for forecasting mission assurance scenarios. This chapter delivers yet another component of the deliverables I had proposed: an empirically based process for rapidly modifying organizational models to incorporate cyber attack effects using SNA derived vulnerability assessments.

The thirty-32 (32) modifications I have described in this dissertation are detail oriented, but are subject to needing reinvention—I would assess that any open-minded operations, logistics, or other similar planner could perform these modifications following the steps of this dissertation. I would recommend pair coding/modeling for future modelers, as it was exceptionally easy to mis-configure the model within ORA as well as the simulation input file (see next chapter for details). I would also recommend future researchers and developers to extend the number and types of scenarios to place under test/forecasting, as well as varying the underlying use case—not all organizations are primarily interested in receiving and processing an operations order, some build widgets, others deliver widgets, others pay the bills for the widget makers.

Simulations

The simulations for this dissertation use Construct, the agent based model simulation discussed at length in the [Overview of Construct](#) section (on page 172). Revisiting the dissertation workflow from [Figure 36](#), we can see where we are in the dissertation workflow by looking at the colored ovals and box in [Figure 118](#).

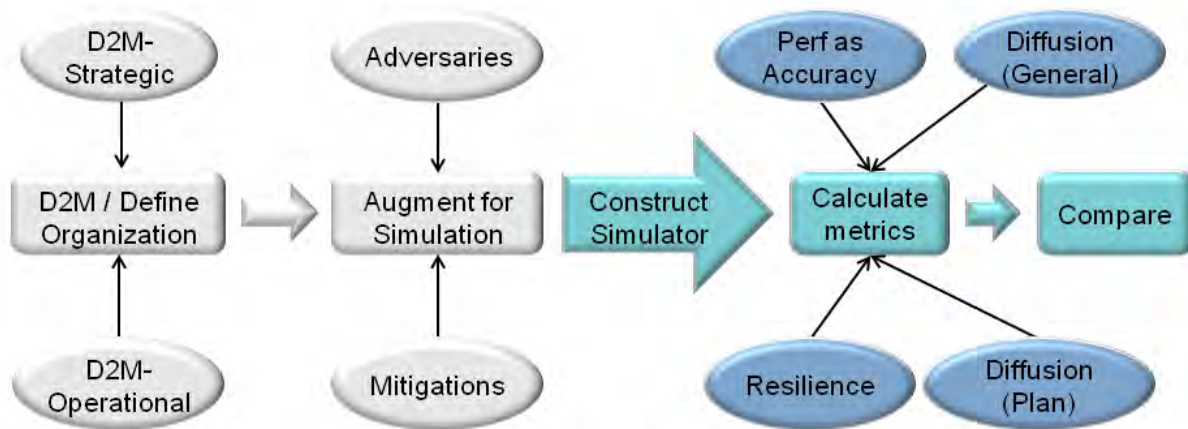


Figure 125 Dissertation workflow executing simulations of models

Before describing the uses to which I put Construct, it is appropriate to discuss some of the changes I put in place, the testing for verification and validation of the changes, and the support I built in for continued maintenance and updates.

Changes to Construct

Construct began in the late 1990s, and has been modified extensively since then by researchers in CASOS and CASOS alumni now at other research institutions. Even with those changes, there continue to be modifications in the code base for purposes of resolving usability issues, aligning user documentation with as implemented functional, adjusting as-designed documentation to reflect as-implemented as well as the reverse. To use Construct for my purposes, to conduct Rapid Mission Assurance Assessment via Sociotechnical Modeling and Simulation, I needed some additional functionality that I have briefly alluded to in previous chapters.

Code base descriptives

When assessing code base complexity, a long-standing, but somewhat simplistic measure of complexity is the lines of code (LOC) in the project. [Table 54](#) below depicts the descriptives created by *cloc*, a perl application (Danial, 2015) of the source code before I and other CASOS developers began modifying it in 2012.

Table 54: Lines of code summary for Construct, pre-dissertation

Language	files	blank lines	comment lines	code lines
C++	71	9,355	14,166	27,519
C/C++ Header	80	4,164	3,615	12,960
CMake	2	472	310	1,605
Sum:	154	14,022	18,097	42,187
Total LOC	74,460			

A second table, [Table 55](#), depicts the combined efforts of source code modification between three authors. My classmate Kenny Joseph is responsible for implementing the Boolean Transactive Memory related modifications to the application. A simple line count for those efforts are included, and then deducted from the total changes observed in the code base.

Table 55: Lines of code summary for Construct, post-dissertation, by Joseph, Kowalchuck and Lanham

Language	files	blank lines	comment lines	code lines
XML (testing input files)	8	622	891	45,769
C++	161	9,549	18,469	31,634
C/C++ Header	172	5,128	5,817	18,854
CMake	3	35	82	115
DOS Batch	2	36	9	116
SUM:	346	15,370	25,268	96,488
Total LOC	50,719 exclusive of testing input files			
Total LOC Change	8,532 exclusive of testing input files			
TMBool LOC	2,536			
LOC Change w/o TMBool	5,996			

I was unable to differentiate Mike Kowalchuck's work as it was throughout the code base. Mike is one the principal staff developers in CASOS, and he had the yeoman's task of incorporating all the many changes Kenny and I created. The changes, grossly summarized in terms of lines added, or removed, are shown below in [Table 56](#). Of note in this table is the im

Table 56: Lines of code added and removed during refactoring and additions

Language	files	blank	comment	code
make				
same	0	0	0	0
modified	0	0	0	0
added	0	0	0	0
removed	1	439	244	1,276
Bash Shell				
Same	0	0	0	0
modified	0	0	0	0
Added	1	33	9	113
removed	1	31	6	103
DOS Batch				
same	0	0	0	0
modified	0	0	0	0
added	1	3	0	3
removed	0	0	0	0
XML				
same	0	0	0	0
modified	0	0	0	0
added	8	622	891	45,769
removed	0	0	0	0
C++				
same	0	0	0	0
modified	0	0	0	0
added	161	9,549	18,469	31,634
removed	71	9,355	14,166	27,519
C/C++ Header				
same	0	0	0	0
modified	0	0	0	0
added	172	5,128	5,817	18,854
removed	80	4,164	3,615	12,960
HTML				
same	0	0	0	0
modified	0	0	0	0
added	4	0	0	821
removed	0	0	0	0
CMake				
same	0	0	0	0
modified	0	0	0	0
added	3	35	82	115

removed	1	33	66	329
SUM:				
same	0	0	0	0
modified	0	0	0	0
added	350	15,370	25,268	97,309
removed	154	14,022	18,097	42,187

Binary Tasks as a motivation for interaction

Part of the deliverable I proposed for this dissertation was a set of modifications that added binary tasks as a motivation for interaction between agents. I achieved this modification through extending Construct code originally written by Kenneth Joseph, placing extensions under a testing framework, and authoring new code.

I added the ability for agents to calculate the binary task similarity and binary task expertise values that are contribute to agents stochastic decisions about who to attempt to interact with. Binary task similarity, much like knowledge similarity, is a score the simulation tracks to support homophily based interaction (that is egos interacting with those alters that are similar). Binary task expertise is the other calculated value drawing directly from the knowledge expertise code base—it is a score on a per-alter basis that the higher it is, the more an alter has binary tasks the ego does not.

The agent x binary task network most commonly conveys which binary tasks each agent is assigned. The agent (ego) x agent (alter) x binary task network is the transactive memory of which alters the agent believes are assigned to which tasks.

Agents can now add binary task assignment bits to their messages they transmit to their interaction partners. In the case of transmitting a bit from the agent x binary task network (the task assignment network listed in [Table 7](#)), this would be the equivalent of the ego agent assigning a task to the alter agent. That is not an intuitive behavior, and I have placed warnings in the technical report for ORA, the source code, as well as the Doxygen comments to warn future experimenters.

Agents can also add binary task transactive memory bits to their messages they transmit to their interaction partners. This is the equivalent of an ego, telling its interaction partner that

one of the ego's alters is assigned to a particular task or set of tasks. This behavior is as intended and as designed for the simulation, and fits well within the literature on why humans tend to interact with each other.

Improve Maintainability

I added copious quantities of embedded and inline comments, explanations, and math functions using syntax geared for ingestion by doxygen (van Heesch, 2014). Doxygen is a program that creates source code documentation and graphical class inheritance diagrams in multiple output formats.

To author and render math functions I used MathJax (MathJax Consortium, 2014) , a JavaScript display engine for mathematics. I embedded Construct's driving equations into the comment structure for classes where significant calculation was a fundamental task. The equations embedded in the code therefore represent an as-built view of Construct's behavior that future readers will be able to compare/contrast to technical reports or user manuals.

Construct Unit testing using Boost:UnitTestFramework

The majority of the files I added to the source base fell into one of two categories: unit test files and refactoring classes into their own files (in lieu of multiple classes in a single header/source file pair). The end state of the dissertation is that I have placed 23 classes under varying levels of test coverage, ranging from 100% to as little as 10% of the public APIs. The principle advantage to this contribution is that future developers can use both the Boost Unit Test Framework (Dawes, Abrahams, Josuttis, & Et. al.) test cases and the XML input files from previous versions to verify their implementations perform as they should and as the older versions of Construct used to.

Table 57: Class count changes in code base

Code base stage	Class Count
Pre-Dissertation	297
Post-Dissertation	324
Class growth	27
Unit Test Classes	23

Analysis

To establish the experimental baseline, and after conducting the augmentation of the model as I discussed in the previous chapter, I used the CASOS Condor High Throughput Computing Cluster ("Computing with HTCondor," 2015). This cluster supported executing multiple iterations per run condition to identify inherent variability in the execution of the model. The variability helps establish face validity in the minds of reviewers as it demonstrates the ability to incorporate stochastic processes into the simulation.

Omitting New Resilience Metric

The analysis of the simulations does not include the newly developed resilience measure. This is principally because in test and initial simulations, there were no observed effects on the measure. Part of the no change result was predicted; the static assessment uses 'resources' while the construct model does not. I had expected some change however since the attack scenarios involve the logical deletion of highly connected IT agent nodes. I expected this would cause the creation of pendants of pendants in the agent chains remaining in the model. I had also expected knowledge bits connected to the deleted agents would contribute to a change in the resilience score. I was wrong. What changes did occur happened in the four and fifth decimal places, and I had to revisit my expectations.

My working hypothesis for this outcome is that the process of augmenting the model for Construct caused the agent node pendants of pendants to no longer exist. Addition of links and joining agents to groups caused them to not be isolated anymore. As to knowledge, if there were any knowledge bits that could no longer diffuse when the availability attack occurred, its loss was not noticed by the organization level measures. Finally, when augmenting and cleaning the data file, especially in my efforts to reduce run times to a manageable duration, I use an automated remove isolates capability in ORA. Because I defined isolates using the entire meta-network ontology, there were still several thousand knowledge bits in the ORA model, not connected to a single agent, though many did form knowledge clusters. Without connections to agents, the knowledge bits were simply causing the simulation to run slower but still could never diffuse. This was also true of tasks. When I deleted isolates from those two individual networks

(agent x knowledge and task x knowledge), I made it even more challenging for the resilience score to change. Given the lack of changes, my conclusion for the resilience score is I have demonstrated its applicability to static models generated from the D2M process. I have also demonstrated that model cleaning and augmentation techniques as well as attack scenario implementations can negatively impact the resilience score calculations.

Instead, I choose to analyze other aspects of performance that help answer the ‘so what’ of the indicated drop in performance we saw in the static analysis. In the static analysis chapter, we saw drops in measures that varied from nearly zero percent (0%) change to 60% and higher. To operationalize the impacts of those measures, the analysis deliberately constrains itself to the impacts to a small sub-set of the simulation population per model. Specifically, I focus on the diffusion of ‘plan’ knowledge in a normal execution environment to the agents that ‘attend’ the planning and plan briefing events in the simulation. An additional operating premise of the dissertation is that sufficient diffusion of ‘plan’ knowledge within key leader population is necessary for adequate execution of the plan. This premise nests with the generalized statement that at the operational and strategic levels, commands tend to be more information-task oriented than other types of DoD organizations. The structure of my experiments and the scenarios that I have chosen are simply one of the many ways future researchers could instantiate a mission assurance simulation scenario.

Diffusion of plan knowledge, operational and strategic

In each of the two models, as shown in [Figure 126](#) and [Error! Reference source not found.](#), the diffusion curves of the plan knowledge have the warm up period on the left of the chart; there is an increase in the rate of diffusion during and after each of the 3 simulated planning meetings. This is most clearly seen in the change in slope at time period 21, the beginning of the ‘planning cycle’ and just before meeting one (1). As noted in the augmentation chapter and even in the visual rendering of resilience from [Figure 2](#), the warm up assists in establishing an equilibrium with respect to agents’ transactive memory being initialized and stabilized, stereotypes generated, and entropy associated with forgetting.

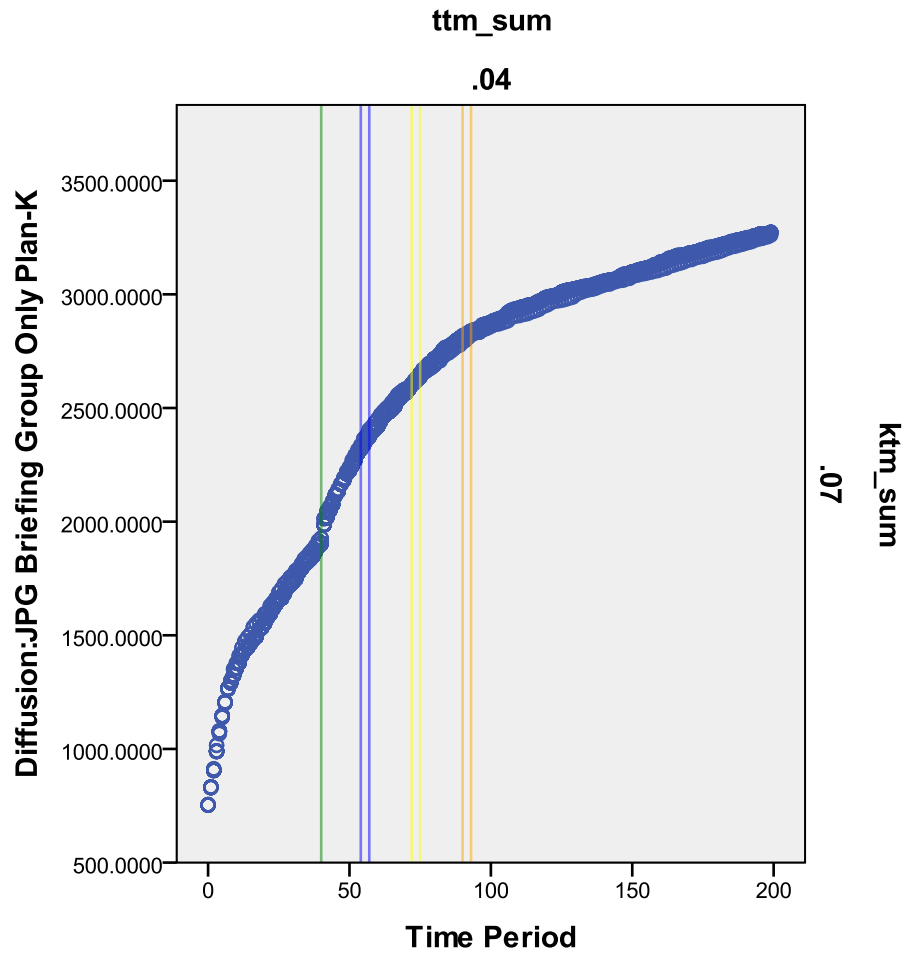


Figure 126: ‘Plan’ diffusion for operational model

$$PlanKnowledge_{\max} = 17 \text{ jpg \&jpg briefing agents} \times \frac{300 \text{ plan_bits}}{1 \text{ agent}} = 5,100 \text{ bits} \quad (49)$$

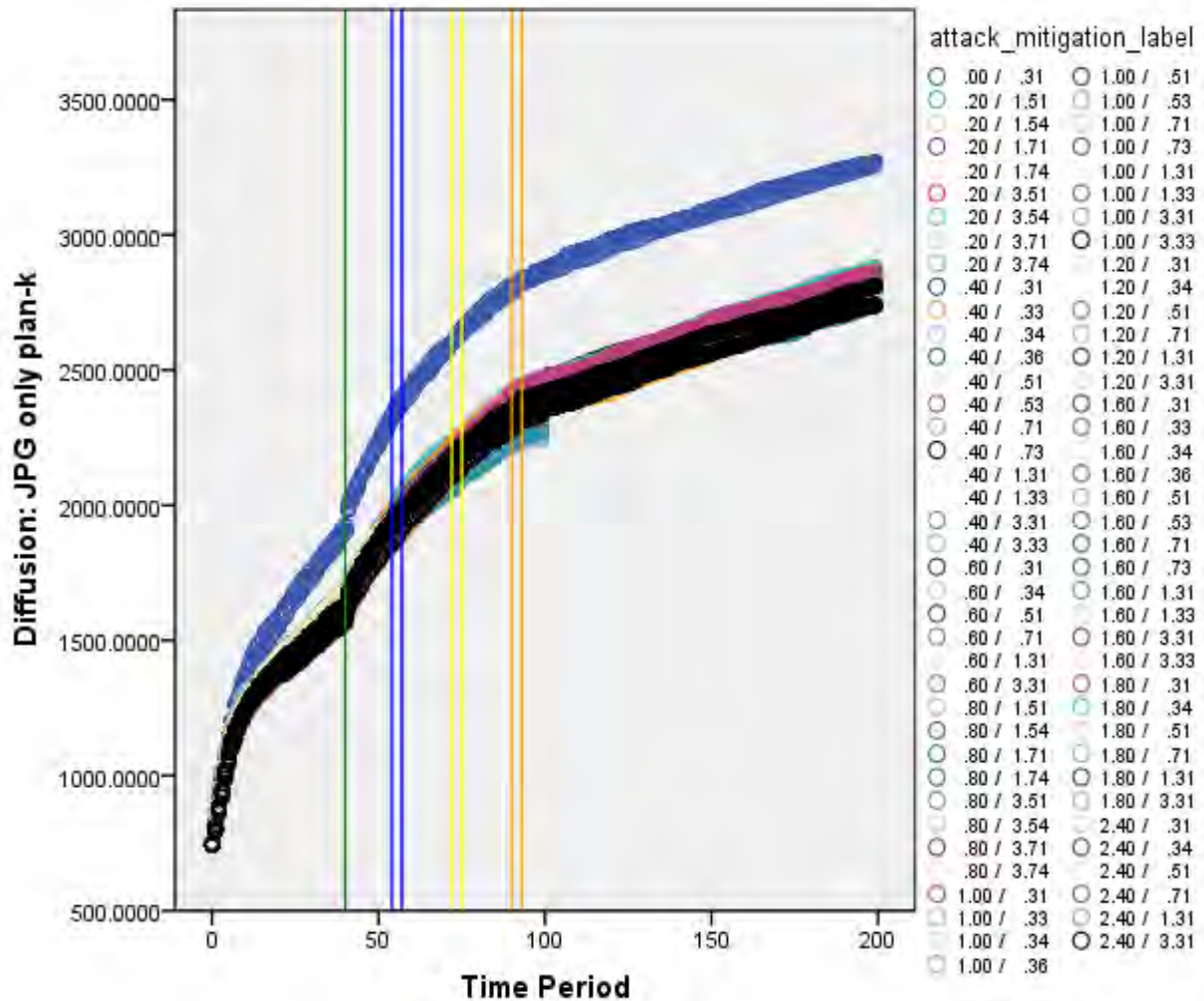


Figure 127: Operational model information diffusion effects for single-vector and multi-vector attack conditions

I had expected the mitigation of reducing the transactive memory error rates to provide a more substantial effect on plan knowledge diffusion that it demonstrated. With a decreased opportunity to have incorrect perceptions, the simulation suggests that newcomer training is helpful in increasing diffusion, even in contested cyber environments. This suggests to commanders that should emphasize initial who-does-what and who-knows-what, at least in the larger organizational sub-groups.

The rise in plan diffusion after attacks in the scenarios where the spares were brought online was, like the strategic model not very pronounced and was barely correlated with the use spares in the first place. This was a surprising result, as I had expected a distinctly visual difference as well as a more pronounced statistical evidence of efficacy. My working hypothesis there are more IT systems with the plan knowledge in these scenarios, thereby helping spread the information at a faster rate and to a larger population.

I had expected and saw a very small increase in plan diffusion by changing the ratio of meeting time to planning time during the planning cycle. The resulting change in diffusion was statistically significant ($p < 0.005$), but miniscule from an everyday perspective and barely correlated (correlation was 0.03, with $p < 0.005$ as well). Though the increase is not dramatic, this particular adaptation has challenges in operational units as it does in strategic units. As noted in the potential leadership interpretation above, too many meetings in favor of planning will reduce the flow of information within the leadership circles.

The 10 dimensional response surface generated by the Box-Behnken design shown in is necessarily inaccessible for visual rendering except in slices and pieces. I have not depicted or discussed outcomes for combinations of factors that do not demonstrate outcomes of potential interest to organizational leaders. This is a useful aspect of M&S based experimentation however as there are little to no differential costs in running additional scenarios—though the same is not true of the analysis efforts associated with each scenario. What this approach supports however is forecasting for conditions that will, or should, cross the risk-acceptance thresholds of organizational leaders. Those leaders can use the scenarios with intriguing or obvious results to guide their decisions to establish training objectives and expectations in their formal training calendars and events. The outcomes of the M&S experiments thus serve as screen criteria for selecting high-payoff scenarios when the unit shifts from simulation to live or constructive training modalities.

Strategic Model

As previous work (Lanham, Morgan, et al., 2011b) indicated, I had expected that the strategic model would experience non-linear changes when confronted with multiple attack vectors. In the figure below the reader can see there are effects, and they follow the same reduction in diffusion pattern as the operational model, but they are not as dramatic as predicted. There are obvious changes in slope during planning periods and meetings, and different maximums achieved for various attack combinations. The vertical bars in the diagram represent the 3 planning meeting periods. The top most series of markers is the average of the best condition (no attacks and very low false positive and false negative rates for transactive memory). There were a total of 46 people in the JPG planning group and JPG Briefing group, with 510 total plan bits, leading to a theoretical maximum diffusion of 23,460 bits I would expect to see in

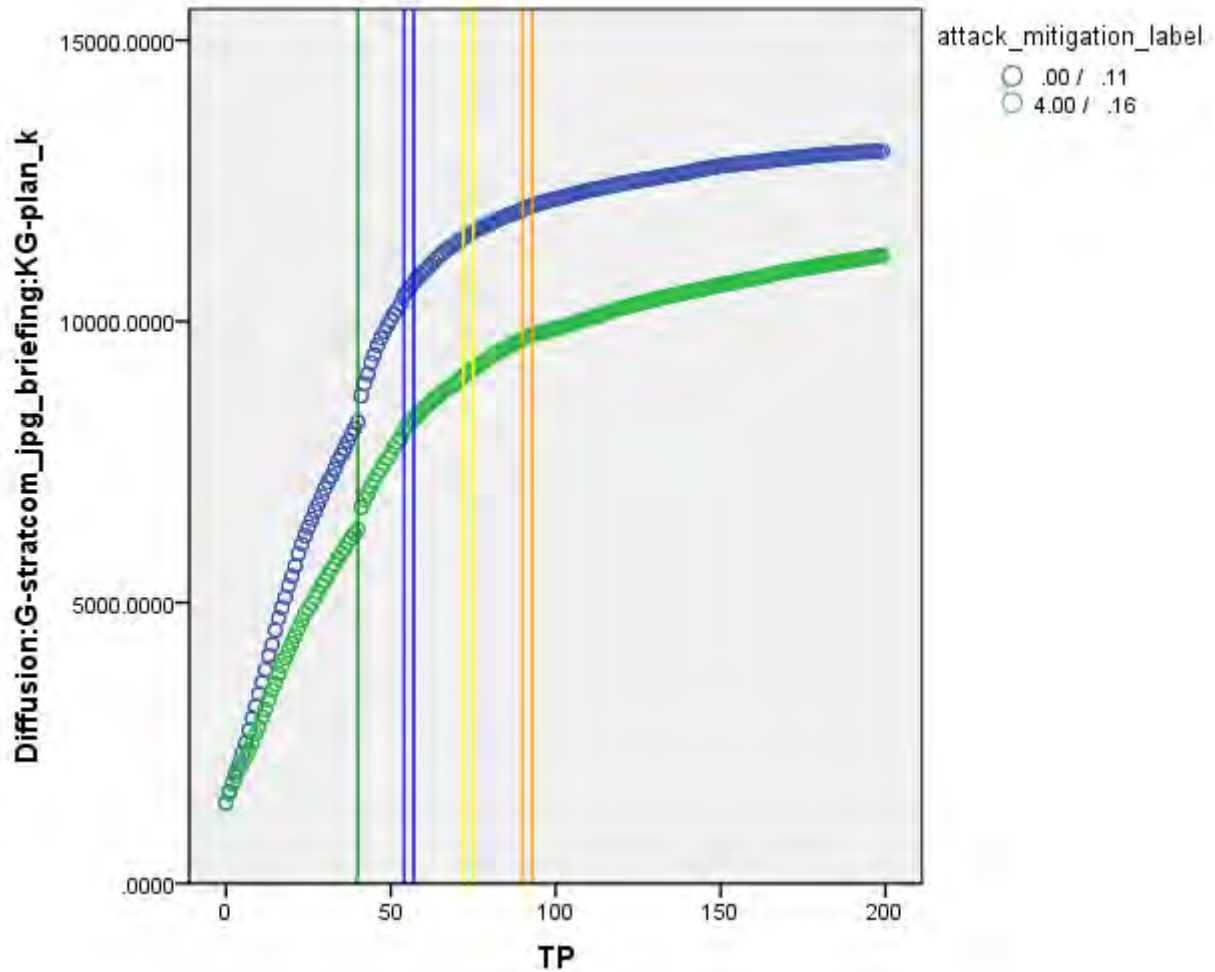


Figure 128: Strategic model best and worst cases only

Performance as Accuracy

Performance as Accuracy is a calculated measure that generalize the alignment of knowledge tied to tasks with knowledge possessed by people assigned to those tasks. This measure, applied to each model in turn, has as its operating premise that alignment of agent-possessed knowledge, agent-assigned tasks, and tasks' required knowledge. The caveat of course is the measure does not offer task-specific visibility to leaders about which tasks, per-se, the organization will do poorly in, it simply offers an indicator of increased probability of higher or lower performance. With that in mind, the two graphs below convey two very distinct outcomes for which I do not have an initial hypothesis. The operational model, across 32 tasks assigned to the various members of the JPG and JPG Briefing groups, had a distinctive pattern to the amount of knowledge the groups possessed for tasks they were assigned. The air_refueling task depicted,

derived from D2M generated extraction processes, has 12 bits of knowledge linked to it. One or more members in the JPG and JPG briefing group are assigned the mission to plan air_refueling in support of other operations.

I had expected a gradually increasing curve depicting a slow growth in the possession of this knowledge. I was wrong. Instead, the pattern depicted in the graph held sway: agents gained all of the bits necessary for a high probability of completing the task very early, and generally held on to them. I assert the turn-by-turn drop and rise is reflective of agents being able to forget knowledge, then re-acquire it.

More interesting was that this pattern was true for each of the tasks assigned to these two sub-populations. The tasks were insensitive to attack conditions, suggesting that the D2M process captured the essence of tacit knowledge within the group: the knowledge is resident in the agents' memories, and they are not reliant on their IT systems as the sole source of that knowledge. The task knowledge was also insensitive to the mitigations. This suggests that the agents assigned these groups rarely have their task-peers fall out of activated transactive memory, else their knowledge would decay through non-use.

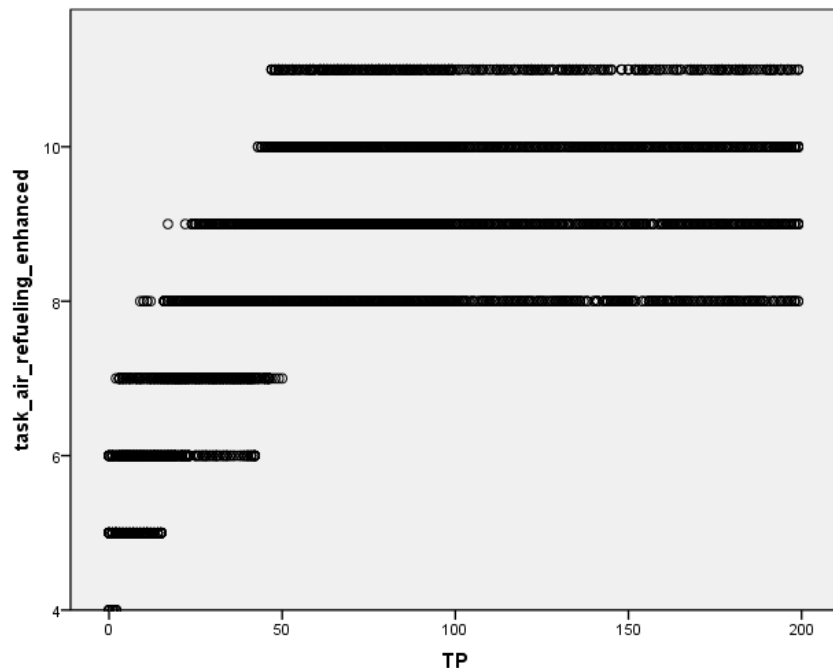
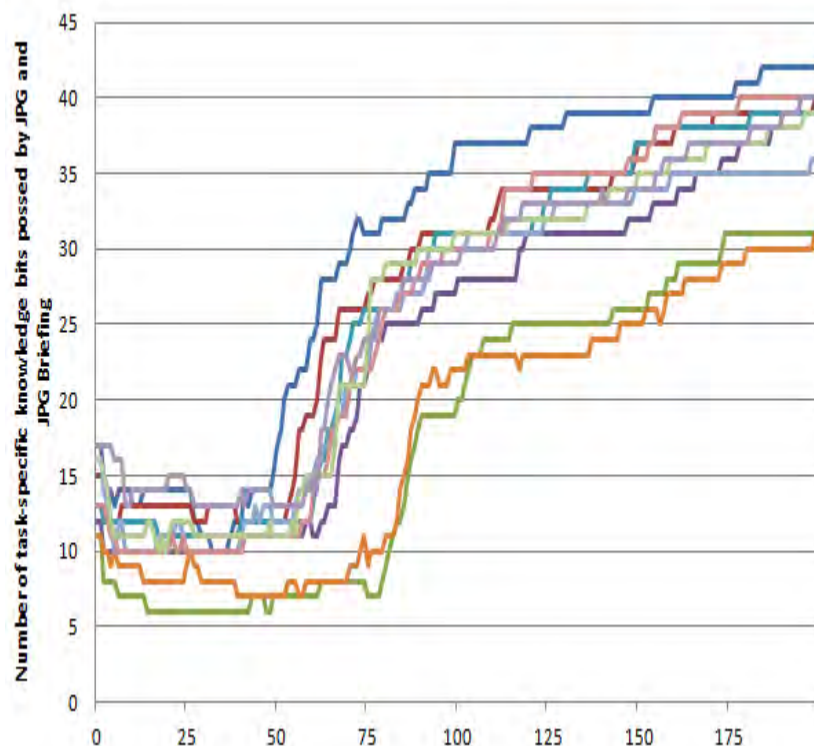


Figure 129: Baseline performance as accuracy for operational model

The strategic model behaved in a very different manner than the operational model, and I do not yet have a hypothesis for why or a generative mechanism for the behavior. The model

behaved as I had initially expected: the number of agents with the task-related knowledge would rise and reach equilibrium, strongly suggesting that for those tasks, the organization has a high probability of correctly implementing the tasks. I had not expected the rise to be delayed as it was, and indeed the initial stages of the simulation saw a slight in access to this knowledge, supporting the need of simulation warm up period. Across all the conditions tested under the Box Behnken methodology, the strategic model demonstrated no sensitivity for these tasks across attack or mitigation conditions.

The insensitivity of both models to the attacks could very well be an artifact of the M&S world, some inadvertent over-circumscribing behaviors and interactions, or otherwise not materially relevant. What it could also be, and is very suggestive of, is that people can and do retain information even when they lose or suffer degraded access to their IT. With practice to reinforce a mindset of resilience, these organizations, and potentially many others, can have confidence that they can accomplish far more in a contested cyber environment than mass media



pontificators suggest.

Figure 130: Baseline reflection of performance as accuracy for strategic model

From this baseline analysis of non-contested environments, I move on to analyzing and summarizing the six attacks in their various combinations as well as the mitigations. Before doing so, I will provide a slightly more in-depth review of the mitigations in place.

Confidentiality assessment

Recall the I modeled a passive confidentiality agent that I connected to ‘level1’ IT systems. My motivation for selecting ‘level1’ IT systems is that the mass media typical reports on compromises of military and company’s systems that are not cryptographically separated from the global internet. Since I’ve not read reports of breaches of classified systems, it seemed plausible to have had an adversary that will have compromised multiple systems, and ideally systems they would consider important. I am not modeling an advanced persistent threat however, as the agent is passive, does not initiate interactions, and the reader can think of the agent as a confidentiality sink.

The assessment of the sink if not operationally focused. Without a specific time, organization, or circumstance, assessing operational impacts to any particular breach is a generalized challenge—possible suitable for its own research area. However, in this case I reviewed the confidentiality agent’s ability to absorb and maintain ‘level 2’ plan knowledge.

I expected the sink to accumulate a small percentage of ‘level 2,’ and expected it to slowly grow over time and possible reach some low equilibrium. I was wrong. The next to figures show the average is highly variable across attack conditions, with two peaks, but not sufficiently so to call the average a bimodal distribution.

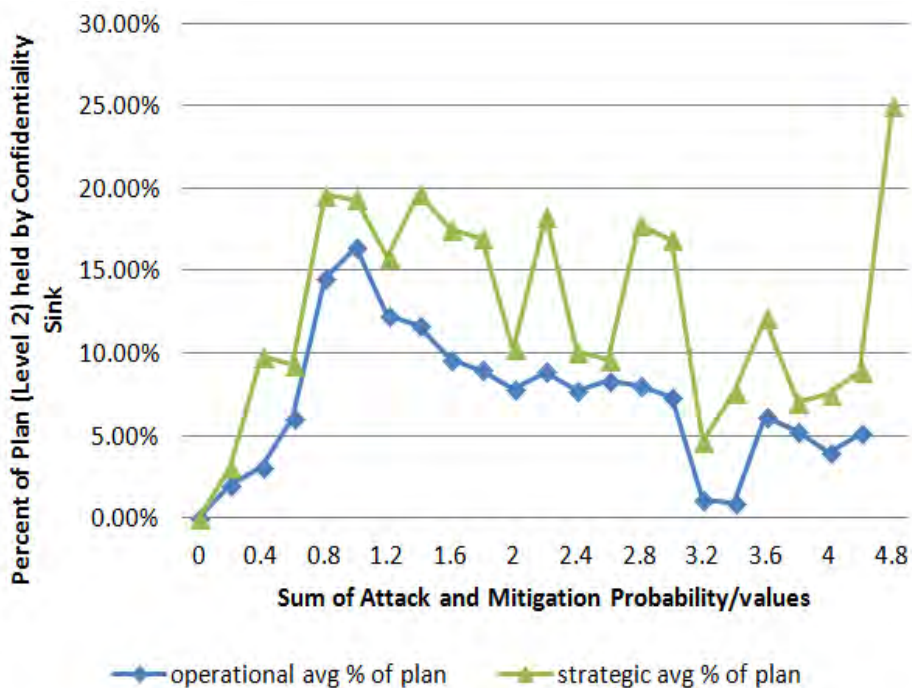
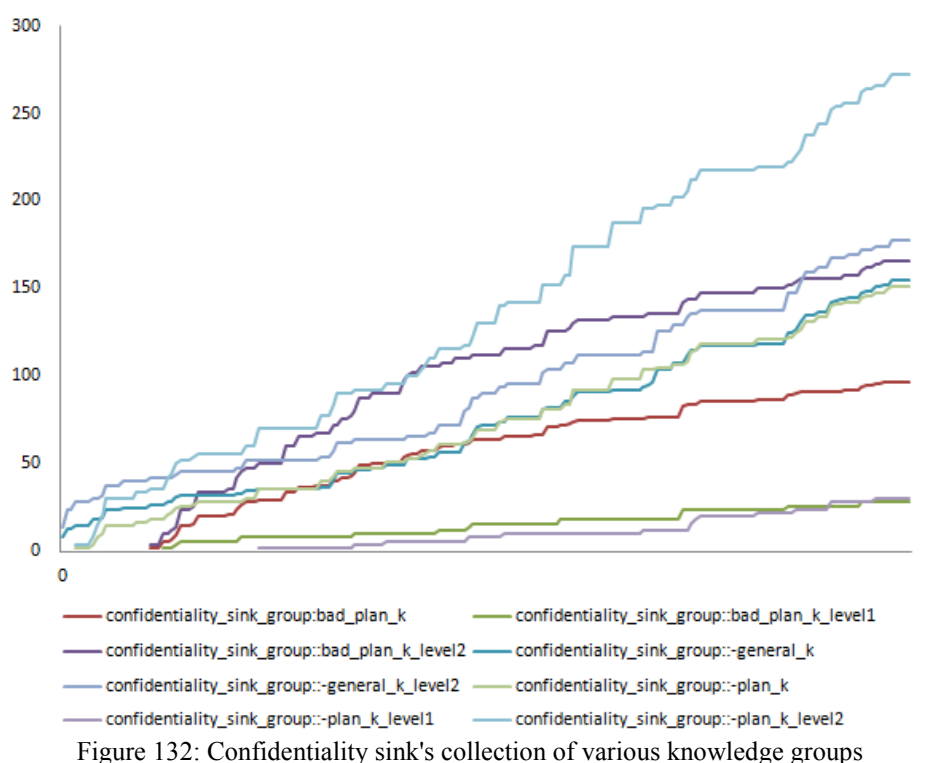


Figure 131: Average plan distribution across attack and mitigation conditions

In retrospect, I should have expected a peak during nothing but a confidentiality attack (at 0.8 on the x axis) as that attack condition has no other competitors or interference occurring in the model. I had not expected the peak at the far right of the figure for the strategic sink agent. In this condition, the sink has attained almost 25% of the ‘level 2’ plan knowledge. This is a surprising amount. I’ll discuss a working hypothesis after reviewing the sink’s ability to collect the other forms of knowledge in the simulation.



In [Figure 132](#), we can see that the confidentiality agent, though constrained by being unable to initiate interactions, nonetheless gathers a significant amount and variety of information. The x-axis is time, with the y axis the number of bits the agent has gathered, with each line representing a different group of knowledge—knowledge groups are exogenous to the agents and for the modelers use in configuring the simulation. In this chart, this not very aggressive passive agent, in the worst case strategic model, is able to get a large variety of knowledge!

Mitigations

New arrival training informs new members of the organization who-knows-what and who-does-what. These correspond exactly with Construct’s ability to implement knowledge

transactive memory and task assignment transactive memory. New arrival training has a history of improving organizational performance (Bartel, 1994) with Tracey et al building the General Training Climate Scale to provide feedback to management (Tracey & Tews, 2005). Within the military, this is akin to a new arrival receiving an overview briefing of the organization with fairly explicit details about what each staff section and sub-section does, as well as learning the names of members in those sections. Learning what the sections do (task assignments) supports individual agents in creating generalized perceptions of all agents in the subsections. By varying the false positive rates and false negative rates for each of the types of perceptions, I expect the modeled organizations to have better performance with low false rates for all four variables.

The second change, use of replica Key IT systems (and their starting knowledge) and varying how fast the equipment is brought online, increases knowledge redundancy within the organization. Redundancy as a means of improving resilience to disruptions is a known technique in multiple fields: public-key cryptosystems (Frankel et al., 1997), design of control systems in critical infrastructures (Rieger et al., 2009), provision of public services (Low et al., 2003), and is frequently seen in functional redundancies in ecosystems (Low et al., 2003). The US Chemical Safety and Hazard Investigation Board (Crichton et al., 2009) widespread distribution of knowledge, especially of past organizational failures, is specifically called out by. The variable aspect of this component is how fast mitigation techniques are fully in effect— analogous to rehearsals that improve the ability of organizations to react to situations.

The last mitigation I experiment with is the varying of the meeting to planning ratio for the JPG and JPG briefing attendees. In time compressed environments, the military already practices something like this mitigation—it is sometimes called an abbreviated military decision making process. Abbreviated MDMPs usually require more participation by leaders (more ‘meetings’) and less time by specialized planners (JPG planning) isolated in their planning cell. increasing shared situation awareness. This technique is also common in the emergency management services (Comfort, 2006). I expected modeled organizations with this mitigation to have better performance than the baseline up to a point, and then I expect a worsening return on investment of leaders’ time.

Both model experienced degradations when confronted with multiple attack vectors, though I was not able to generate the non-linear effects seen in previous work not in the static assessments.

I was also unable to generate, despite literature suggesting otherwise, significant improvements with the mitigations I experimented with. In both models, the improvements were statistically significant ($p < 0.005$), but in my assessment not meaningful or significant to the average commander. Of course, a 3-5% improvement to one leader in one organization may be a ho-hum response, while another organization would find that level of change an emotional event. None of the observed changes are as obvious as I had predicted in either graphical or mathematical model form.

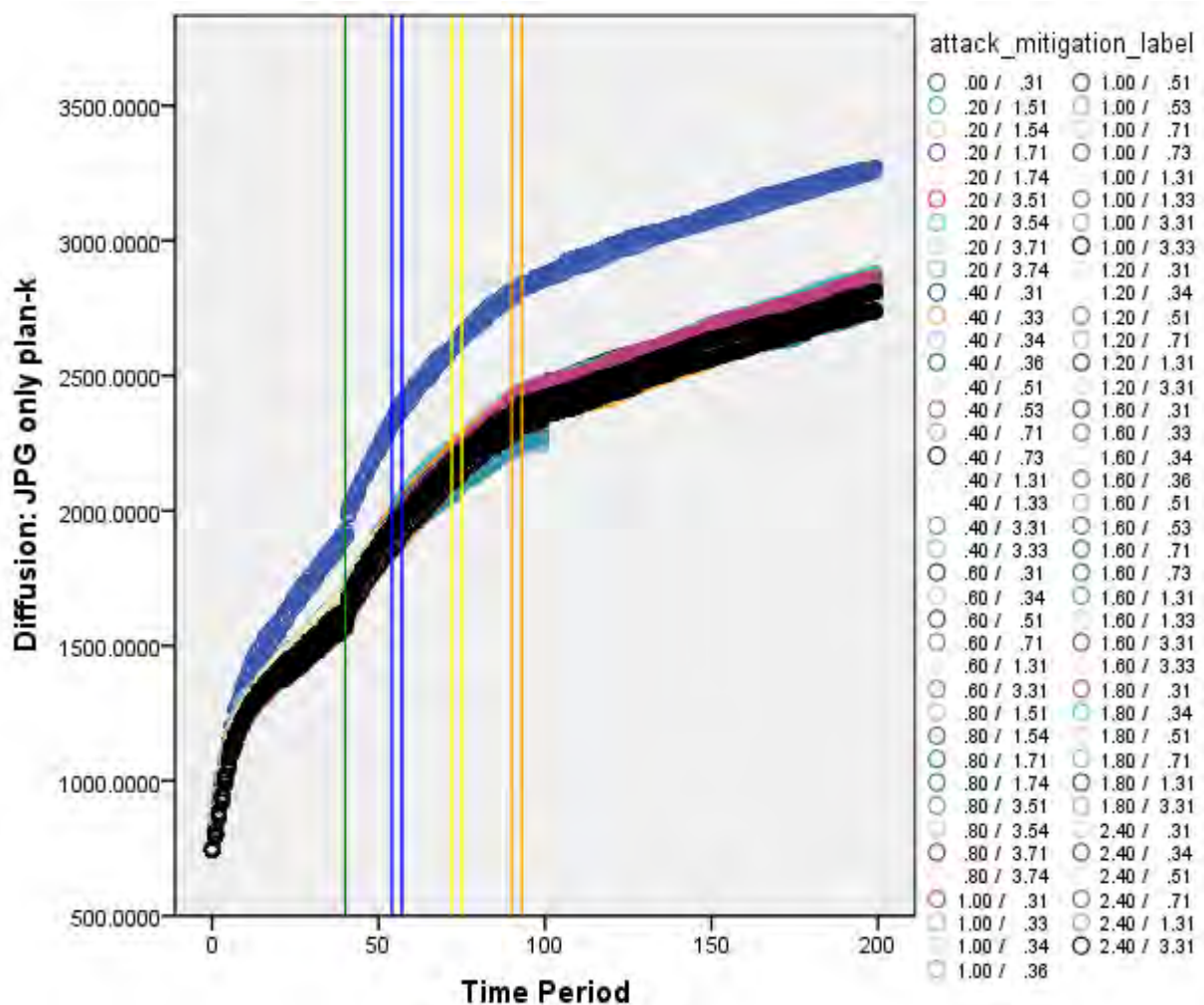


Figure 133: Operational model information diffusion effects for single-vector and multi-vector attack conditions

Revisiting the diffusion graph, the legend to the right of the figure remains the sum of the probabilities in effect (since rendering a graph along 10 dimensions is impractical). The label “0.00 / 0.31” indicates there are no attacks in effect, and the lowest false positive and false negative rates are in effect for transactive knowledge memory and transactive task assignment memory. The figure depicts that none of the mitigations are profoundly good at reducing the impacts to the attacks. This was not as expected, though it certainly gives credence to the thought that M&S will need to explore the universe of good ideas before leaders commit precious resources with artificially high expectations of preparations and mitigations.

There is sufficient information in the graph though to allow organizational readers to interpret the figure in this way:

The organization as modeled can, on average, disseminate over 70% of the plan to the members of the JPG Briefing group. When put into a contested cyber environment of DDoS, the organization can expect to drop in performance, on average, 16%. Combined, this means the organization can reliably say 60% of the plan will reach the senior leadership of the organization.

*There is a band of performance the organization will need to refine and explore to decide how best to improve overall dissemination as well mitigation efficacy. No mitigation under test restores the organization to its pre-attack effectiveness. The organization itself does not return to pre-attack effectiveness with respect to **this** planning cycle and **this** planning task for **this** attack..*

A hasty dive into the underlying data shows that exceeding 0.40 as the ratio between meetings and planning, induces a reduced dissemination effect, which is congruent to the 1/3 2/3 rule the DoD uses for staffs and planning- time allocation.

I had expected the mitigation of reducing the transactive memory error rates would provide a more substantial effect on plan knowledge diffusion that it demonstrated below in [Error! Reference source not found.](#) Indeed, the surprising aspect of the false negative rate was that it was negatively correlated to diffusion success, albeit very slightly. The false positive rates however were positively correlated ($p < 0.005$) with better diffusion rates. This suggested that newcomer training geared to providing specific information about who-does-what and who-knows-what is helpful in increasing diffusion, even in contested cyber environments.

What I had not expected was the rather dramatic rise in plan diffusion after attacks in the scenarios where the spares were brought online. As seen in [Error! Reference source not found.](#), the plan diffusion curve is a definite improvement to the no attack condition as well as the pre-attack condition. My working hypothesis, and in retrospect predictable outcome, is that there is simply more IT systems with the plan knowledge in these scenarios, thereby helping spread the information at a faster rate and to a larger population.

I had expected and saw an increase in plan diffusion by changing the ratio of meeting time to planning time during the planning cycle. Though the increase is not dramatic, this particular adaptation has operational challenges in units. What it effectively does is requires a large percentage of key leaders in the organization to decrease their attention and effort spent on their other duties. This worked fine in this scenario, but would likely cause many a commander to have second thoughts on doing so as a long term solution.

Heuristics

This chapter is an opening effort at distilling tens of pages of detailed analysis to heuristics for consumption by organizational leaders. Like all heuristics, their value will come from their general accuracy, their brevity, their references to other experiential frames of references, and their adoption. Some of the heuristics below are not directly supported by the evidence of this dissertation, but are extrapolations of experience and intuition. The very need for extrapolation is evidence of the continuing gaps in research and experiential learning.

First and foremost, to paraphrase a co-worker, military cyber space operations are traditional military operations on non-traditional terrain (Lanham, 2012a). Removing the military context, cyber space operations are traditional business operations in non-traditional regulatory and market environments. Moderately stripping away the aura of uniqueness and specialness of the IT-realm can enable leaders to recall their other professional planning and coping skills while avoid the pitfalls of disaster mythologies (Tierney et al., 2006). This rule of thumb is especially important and seen in practice during community reactions to natural disasters (*Coping with Catastrophe: Building an Emergency Management System to Meet People's Needs in Natural and Mammade Disasters*, 1993; Quarantelli, 1988; Reason, 1991): leaders that retain a semblance of calm under stress help the community maintain its sense of capacity to overcome adversity. In the military context, there are few scenarios where professional militaries will surrender or otherwise stop military operations simply because of setbacks and adversity nor would they tolerate leaders who refuse to plan and rehearse for obvious eventualities.

Legal authorities matter, as they do in traditional military and business operations. Espionage and warfare are lawfully different activities; as a nation, we do not habitually use the military to conduct espionage, nor do we use espionage agents to conduct combined arms military operations. Conducting everyday business and industrial espionage, sabotage, or counter-sabotage are also all different activities, controlled by differing legal frameworks, regardless of individuals personal opinions or beliefs. Combining these two heuristics leads to the following logical assessment. Military cyberspace operations are not inherently extensions of cyberspace espionage any more than coalition and multi-service maneuver and clash of armed forces are inherently extensions of covert operations.

Small well chosen targeted system losses can affect organizations as greatly as large random losses. Effects vary greatly by system(s) and duration of event(s)/outage(s). Of the twenty MoIs presented in the The tables above support the original assertions that the ideal information processing resilient organization should have no near isolates, maximal excess knowledge and resources (e.g., twice what is minimally necessary), and no needs. They also show that the least resilient organization is hyper-efficient in knowledge and resource distribution with no waste whatsoever. The least resilient organization also has the degenerate case that all tasks, resources, and knowledge are near isolates and accessible only through agents that are pendants. Finally the least resilient organization has every task short of necessary knowledge and resources. These assessments fulfill the third challenge of organizational leaders: identify their organization's structural vulnerabilities.

The next section begins addressing the fourth challenge for leaders, being able to forecast mission assurance scenarios.

Entropic and Targeted Attacks [The tables above support the original assertions that the ideal information processing resilient organization should have no near isolates, maximal excess knowledge and resources \(e.g., twice what is minimally necessary\), and no needs. They also show that the least resilient organization is hyper-efficient in knowledge and resource distribution with no waste whatsoever. The least resilient organization also has the degenerate case that all tasks, resources, and knowledge are near isolates and accessible only through agents that are pendants. Finally the least resilient organization has every task short of necessary knowledge and resources. These assessments fulfill the third challenge of organizational leaders: identify their organization's structural vulnerabilities.](#)

[The next section begins addressing the fourth challenge for leaders, being able to forecast mission assurance scenarios.](#)

[Entropic and Targeted Attacks](#) starting on page 150, percentage change impacts were as low as 0-1% at 10% loss levels (random) to as high as 80% at 75% loss levels. Those percentage change can be a gross form of impact assessment, short of specific organizational impacts with SME-input (or experience), it remains a useful data point for leadership. With those caveats, the table below summarizes the impacts of random losses. The table is akin to the green, amber, red,

black color coding schemes traditional military commanders use for assessing overall operational capability of an organization (see also [Figure 117](#)).

Table 58: Effects of random losses table

Random Loss Level	Operational Impact for Organizational Leaders
Up to 15% random loss of IT agents and IT resources	Little to no operational impact on the 20 assessed SNA measures.
Up to 30% random loss of IT agents and IT resources	10% change threshold crossed on some of the 20 assessed SNA measures
Up to 50% random loss of IT agents and IT resource	Changes are highly variable and range from little to no impact to changes up 60% on the 20 assessed SNA measures
Up to 75% random loss of IT agents and IT resource	Changes are highly variable and range from moderate (>10%) to severe impacts on the 20 assessed SNA measures.

A more nuanced heuristic for the above table is that ‘it depends’ on the MoI, the effected system(s) and the operational impacts. For a hospital, the degradation of a centralized patient database, with no spares or failover capability, could dramatically effect sustained care while the health care providers revert to paper-based systems. The decision to revert would clearly be driven by an estimated time for return to service as well as assessments for any data integrity loss (e.g., corruption of patient data). For time sensitive targeting, organizations may lose small windows of opportunity (Pflanz & Levis, 2012), causing a reversion to other processes or other expectations. For strategic and operational logistics, degradations to business-to-business communications with commercial shipping, rail, and trucking companies may prove inconsequential for short duration events, and could impact controlled supply rates and restricted supply rates for specific classes of supply.

The table above is table, and the more nuanced answer are both aligned with the first paragraph of this chapter. A traditional military commander at the operational level would have an experiential and intuitive basis for knowing that a random loss of 15% of her aircraft may be very consequential of the 15% overlaps completely with a high value airframe. Or the logistician that understands the random loss of the sole material handling equipment at an airfield has ripple effects larger than a single piece of equipment loss would usually generate. Traditional business and military operations require risk mitigation, as does cyber space operations. Traditional

military studies also strongly alternate, contingency, and emergency plans as well as rehearsals of the switch over and execution of those plans.

There is danger in assuming that resilience to everyday outages and challenges equates to resilience to deliberately contested cyber environments. The specific targeting of systems by a malicious adversary will be attempting to create effects within the targeted organization's operations, leadership decision cycles, information flow, or some other goal. The research shows that combinations of key node losses can rapidly shift to non-linear effects disproportionate to the number of systems directly affected. In these models, deletion of as few as ten (10) nodes, when carefully selected, can create effects as large as a random loss of 50% of the nodes. For strategic and national level commands, who perceive themselves as reliant on up-to-the-minute information flow to make decisions, this argues that they should prepare for and rehearse degraded communications!

The paragraph above reinforces the first takeaway of the dissertation yet again. Traditional military operations seek to identify and target adversaries' centers of gravity and decisive points. Such targeting helps set the stage of cascading successes by the friendly elements while depriving the adversaries of decision space and time. The loss of key leaders in an organization can have a disproportionate effect on the workers and processes. Likewise, the creation of an effect in a key leader's world view, can dramatically affect the organization—a deliberate injection of erroneous data to a key leader or key IT system can rapidly and persistently corrupt the decision making and processes within an organization.

The clearest example of this degraded information flow is in [Figure 110](#). An adversary can, in these models, double the amount of time it takes for information to flow through the organizational models. In this figure of these two models, the loss of a single IT system can degrade communications flow up to 10%. Deliberate targeting by an adversary of just 10 IT centers of gravity can degrade IT-only diffusion by 50%, hence the doubling of time to move information. That time lag may be without effect, or it may place national decision maker(s) well outside their comfort zone for decisions without up-to-the-minute current data or information. Expectation management for impacts pre- and post-event is essential to ensure leadership demonstrates resilience in the face of information addictions not receiving their periodic updates.

The table below reduces the content further with the commiserate risk of over simplifying and under stating the variability of outcomes.

Table 59: Rules of thumb for impacts

Cyber Condition	Operational Impact for Organizational Leaders
Random and everyday losses != targeted or deliberate losses	Extrapolating from everyday random losses and typical troubles of ‘build, operate, and maintain’ mission to a malicious adversary imperils assurances as there is no confidence in coping plans
Contested cyber environments will happen	Org leaders and members having estimates of impacts avoids disaster myths, knowing how to adapt and approximate path for return to normalcy is essential to mission assurance
Up to 15% random loss of IT systems	Little to no operational impact—usually Akin to: if luck favors the adversary, loss of a main supply route
Up to 30% random loss of IT systems or Loss of a single ‘key’ IT system	Slight operational impact—dependent on which 30% of the population is affected Akin to: Loss of high level ‘key leader’ contingency requires succession of command plan and expectation of resilience
Up to 50% random loss of IT systems or Loss of up to four (4) ‘key’ IT systems	Moderate to severe impacts without Primary, Alternate, Contingency, and Emergency (PACE) plans in place and rehearsed. Impacts are highly variable! Akin to: Loss of an entire command group or other cluster of key personnel or resources.
Up to 75% random loss of IT systems or Loss of up to ten (10) ‘key’ IT systems	Moderate to severe impacts PACE plans in place and rehearsed. Akin to: Doubling time it takes to move reports across the organization(s). Loss of an forward airbase or port in a theater of operations

The most important take away from this chapter is that the rapid modeling process of the previous chapter can generate an model subject to analytic efforts that demonstrates a recognizable, though nonunique, outcome: targeted removal of IT systems and IT resources in complex sociotechnical organizations can lead to effects disproportionate to the number of directly affected systems and resources. This trend leads to a lesson for organizational leaders that the risk management community has incorporated for a very long time: identify the most important systems and resources and ensure their continuity of operations at some *a priori*

acceptable level. The decision process that identifies those important functions and capabilities can use the techniques in this dissertation as a mechanism, as well as supporting or supplemental means—the key is the realization that a few well-chosen losses will predictably have outsized impacts! This phenomenon has earned the moniker ‘black swan event’ in some circles though it is by no means the only descriptor.

Limitations and Future Work

Text-mining as basis of organizational modeling

There is clearly a prima fascia case for using documentation nominally describing an organization and its workings as the basis for constructing a model of the organization. Unfortunately, the relevant literature on organizational modeling does not address this technique on any consistent basis. This lack of discussion points to gap in applied research toward rapid model construction and a form of rapid model validation—a funding challenge compared to pursuing original theoretical research. The research questions currently open would be approximately, “Does mapping of concepts within sets to ontological categories create consistent meaningful distributions that support researchers’ efforts at validating the ‘accuracy’ of those mappings?” If the answer is yes, a follow-on question could be, “How small a corpus can an organization use to establish a defined confidence interval (e.g. 95th percentile) of capturing meaningful nodes?”

As alluded to in the [Literature Review](#) portion of this dissertation, starting on page 11, as well as the comparisons of edit-cycle 0 and terminal models generated in the [D2M process](#) (see also [Figure 37](#) and [Figure 38](#)), there is a current lack of empirical data for multi-domain ontological distributions. An approach to resolving this lack of empirical data is not hard to envision, and I look forward to pursuing such data in the future. I currently envision a detailed analysis of each input file across the chosen sets, with pre- and post cleaning collection of data, processing times, outputs, and pre- and post processing decisions. I foresee the output of interest being the distributions of the metanetwork ontology per megabyte of input. With those distributions, a future research could, with better mathematical certainty, assert their inputs are representative of the population, as well as their post cleaning results fall within a known standard-deviation from norms. Clearly the choice of ontology would impact the mapping and distributions of concepts to ontological categories. Unless and until sufficient empirical data is available across multiple domains, its infeasible to assert that the distributions evidenced in this dissertation reflect ‘truth.’

Limitations of doctrine and written products as the basis of models

Doctrine and other written products have several obvious shortcomings as the basis of models of specific organizations. Joint doctrine is authoritative within the DoD but is not

prescriptive. Organizations and leaders have the explicit leeway to deviate from doctrine—frequently causing doctrine to be a common point of departure. There is apocryphal story that an American adversary complained that studying American doctrine was useless, as the Americans do not read their own manuals or feel any obligation to follow their doctrine. Though it is a stretch to assert that doctrine is honored more in its being ignored than followed, it is also a stretch to assert that the DoD religiously adheres to its doctrine.

Organizations' written documents can help reduce the disconnect between the way the organization writes about itself and any doctrine/documents that others write about it. Those written documents, depending on their nature, can also help reduce the disconnect between the present day (assuming the documents are of recent generation) and the time when the document was written.

Doctrine is also slow to change or evolve in response to current or perceived futures. Generally, it attempts to overcome this known trait through leveraging the 'authoritative but not prescriptive' caveat within the DoD. This slowness to change can contribute to perceptions that any model derived from doctrine will not be applicable to current-day environments and situations. The slowness to change can also lead to some elements of DoD publishing doctrine that contradicts but cannot outright supercede existing doctrine. There are examples throughout American military history of competing camps of authors and personalities publishing materials that are not congruent with each other. For multi-author documents, it is also possible that documents are not internally consistent with each other. This research effort did not attempt to identify any such contradictory or non-congruent sentiment between the 100+ harvested documents. Adjusting the D2M process to reflect sentiment would be a necessary step to supporting some alignment or non-alignment assessment of the corpus.

Doctrine or other organizational documents also implicitly start shaping bias in the resulting models. Bias could be from internally inconsistent documents as I discussed above. Bias could also derive from the selection of documents to input into the D2M process. I deliberately chose a broad spectrum of documents about joint, strategic and operational military topics. I left out documents dedicated to the use and employment of indirect fires, strategic and operational levels of global logistics, planning and implementing medical support to military operations, defense support to civil authorities and many other hundreds of documents. I

especially left out the hundreds of USG and DoD level documents explicating the various cyber security visions, postures, guides, plans, and other such specialized knowledge.

Leaving these documents out helped me avoid the biasing of the corpus to much toward specialization. Future work is called for though to identify at what cost did I bias the sample? Do input corpi require the same number of sources for each sub-group of interest? Would bias be reduced by using the same quantity of megabytes of input, words, or pictures to reduce quantitative bias through excessively specialized inputs? This discussion of bias also links with the recurring discussion of context to cyber assessments. No researcher should build a corpus of documents about strategic and operational medical operations for wounded troops and use it to build and test hypothesis about non-medical operational planning.

Cyber effects vs. methods-of-attack

This dissertation has not directly modeled the various technical or natural methods that can create a contested environment. Instead I have used the information assurance ontology of confidentiality, integrity, and availability. This means my models do not include a motivation by agents that cause problems nor do the organizations have a perception of cause on the part of their agents. Including a perception of cause, or motivation, is an area of organizational adaptation that is ripe for exploration and analysis—intuition suggests potentially different adaptations to nature-caused effects versus adversary-caused effects. There is also potentially different adaptations or mitigations for adversary-caused effects and the vagaries of modern technology—between a suspected human insider spy and a technology-fault leading to data corruption within a database.

Modeling and Simulations

Emotive responses by agents during events

In none of my scenarios, or even in Construct itself, do any of my agents experience any steady or rising level of ‘frustration’ when they are unable to interact with their first choice or discover their interaction has been obviated by the failure of a communication mechanism. It seems safe to assume that emotional reactions to natural-event driven disruptions will vary from those reactions to suspected or known hostile actions.

There is significant evidence that in communities that suffer natural disasters, the expectation of return to some level of normalcy is key to resilience—in the information deprived environments the seeds of maladaptive outcomes are sown.

The other form of knowledge the agents do not possess, nor are currently designed to incorporate is knowledge that they and/or their organization is actually under attack. The absence of such knowledge is consistent with many real life reporting—knowledge of a breach or attack gets known well after the initial effort began. However, throughout the dissertation, especially in the related literature section, I have talked about perceptions being very important to organizational performance. An organizational reaction to an attack (e.g., deliberately invoking a high cost mitigation plan) may be very different than coping with a natural event such as a storm or even an anchor breaking a cable off the coast.

Future scenarios could not only change Construct agent's awareness of a threat (possibly coded as a belief), but use that belief as a driver of actions seen in companies that have been attacked. I am confident there will be different interaction patterns, which presumably will affect the MoIs used in this dissertation.

Inclusion of more D2M-ontology categories into Construct

'Beliefs' from D2M ontology better carried into Construct

Related literature already exists to support the assessment that agents' beliefs contribute to a sense of likeness, or homophily (M. McPherson et al., 2001; Ridgeway, 2006). The extension of Construct to include beliefs would open the possibility of studying belief-influenced behaviors. Of particular interest to me would be application of beliefs to compliance studies in cyber security. I have a strong intuition that rules without supporting beliefs in the rules' efficacy or applicability are counter-productive to the end-states the rules had intended to achieve. Compliance studies exist in a number of fields from sector specific EU studies (Börzel & Knoll, 2014), providing health care (Rydenfält, Ek, & Larsson, 2013), public administration and red tape (Bozeman & Feeney, 2011), but there appears to be a dearth of compliance studies related to cyber security and incorporating modeling and simulation. I am most interested in research questions that acknowledge humans are the biggest attack surface of any IT system, and whether and how influencing their behavior interacts with technology-focused security efforts.

‘Events’ from D2M ontology carried into Construct

Extending and expanding the forecasting abilities of Construct to a larger set of events would also be a very useful avenue of research. Forecasting future events, the possible impacts of those events on measures of interest, and organizational responses to those events is essential mission assurance as I depicted the concept in [Figure 1](#).

It is not entirely clear to me whether the semantic concepts of events that the D2M process can harvest are translatable into forecastable events. But even if the D2M generated ‘event’ nodes are not good candidates for specific event modeling, there is a large set of possible events that could reasonable form a body of M&S researcher scenarios.

An alternative way of incorporating D2M harvested events is to use them and agents linked to them as drivers of shared-experience interactions. Such an extension to Construct might fall under the umbrella of trust building and interactions with trusted persons for human agents as well as supporting the ‘trustworthy’ belief between egos and alters.

‘Roles’ from D2M ontology carried into Construct

Modelers and researchers can already use Construct to model implicit roles such as boundary spanners, leadership at the top of hierarchies, and other structural definitions of roles. In this conceptualization, I am leaning more toward the differentiation humans give to our various professional and personal roles.

Professional roles within the DoD could be as broad as personnel categories (e.g., general officer, field grade officer, company grade officer) or as specific as work roles (e.g., chief of operations, executive assistant). These roles place implicit, and sometimes explicit, constraints and limitations on decisions by agents. In Construct as implemented, agents have no ability to perceive their roles nor the roles of other organizational members. The D2M process already captures some of the agent x agent links represented in these work specific roles. Having a M&S based implementation of one or more role-based behavior pattern generators would open the door for additional research about whether particular roles are more or less resilient to contested cyber space operations. It could also incorporate lessons from resilience studies of communities and community leadership to negative events (Norris et al., 2008).

A second way of potentially incorporating social roles into future work is incorporating the duality of at-work behavior and away-from-work behavior. This is a direct extension of the

role discussion in the previous paragraph, as organizational members at work have different motivations for interacting with organizational members, than when they are away from work. Family and non-work social interactions, even if they share common motivations (e.g., homophily), the factors used to assess the homophily change—even if the resulting patterns do not.

‘Resources’ from D2M ontology carried into Construct

Task execution in Construct is accomplished in one of two ways: knowledge based decision making (e.g., binary classifications) or energy tasks (not used in this dissertation). Though it is not immediately apparent whether a bolt-on module could be added to Construct to incorporate resource-based tasks, it would certainly broaden the perception of face validity for organizations that conduct activities other than information sharing and processing. Such a bolt-on module would, ideally, be able to directly use the resources identified during the D2M process, as well as the linked nodes to those resources. Resource acquisition could then become its own motivator for interaction, as well as resource acquisition in pursuit of accomplishing resource based tasks.

Circadian rhythms carried into Construct for human agent interaction patterns

Circadian rhythm incorporation within Construct could conceivably assist modelers in developing more complex representations of organizations, should such rhythms be value added. It would require the concept of turns in Construct to become less broad in the general sense, and need to be a selectable option in any case. As currently implemented, each turn can represent as much or as little of real time the modeler assesses is appropriate. Modelers can also divorce real time and its passing from any overt representation in Construct models—an especially useful ability when there is too little empirical evidence to support initial configurations of rates of changes.

Lively and Stale ‘Knowledge’

I created several groupings of knowledge within both models to support simulations and context-based analysis. I also presumed that the plan knowledge was more short-lived than the general knowledge that I code the D2M-identified knowledge and designed the simulation such that plan knowledge could go stale, or be forgotten, faster than general knowledge bits. Plans however vary, and there are different time horizons for various plans even within the same organization.

One such example could be a time-sensitive targeting situation where the weapons release authority is at the strategic or operational level, rather than a tactical level. In such a scenario and use case, the MoI is the ability to execute the targeting process within the time constraints that the organization cannot control (e.g., the adversary is moving from point A to point B, and only accessible in a small time window). This modeling approach, at present is not suited for such a process and time sensitive effort. The success of such a process is more dependent on the technical capabilities of the targeting and flight control systems of the munitions as well as the nearly point-to-point information transfer of target details to lawyers and commanders to decide whether to engage the fleeting target. However, Pflanz performed work at GMU that used colored petri nets to model the process architecture that has no need for cognitively limited agents (Pflanz, 2012). Though we have not conducted multi-model modeling for this scenario, CMU and GMU have conducted virtual experiments in other contexts where the outputs of Construct and Pythia (the Pflanz tool) were congruent with each other.

Additional forms of attacks and effects

I have previously asserted there are many types of mitigations that this method can support assessing. It can also support additional forms of attacks and effects that I did not perform, but are easy to envision.

These additional attacks could be variations on a theme, targeting the IT systems of the organization. They could also be multi-staged attacks where the cyber attack is simply a means to an end. One such scenario could be a compromise of confidentiality of the HR systems that contain agents' contact information, personally identifiable information (PII), or maybe even health care providers database(s). The MoIs I presented in this work are not immediately applicable to such a scenario, but it would seem improbable there would be no operational effect within the psychological operations domain. Such a breach may also support a very fine grained attack along phone lines blocking communications, SMS text messaging of cell phones of employees or their loved ones, or other ways of actively attempting to degrade mission focus. Mission focus could very well be one of the emotive responsive I mentioned earlier in this section as well.

Another form of a DoD computing asset would be the DoD's increasing effort to employ cloud computing and local caching of data to support cloud segmentation. One instantiation of

this is the Army's use of DISA's Enterprise Email, housed in several major processing nodes around the US and in select places of the globe. Cloud computing has as its most fundamental principle uninterrupted network access between the users and the various data centers that house and replicate the IP-based services. These centers' designs incorporate their own contingency plans for various risks but the using customer is still constrained to their small set of communications links and terminals to take advantage of the remote centers. The availability attacks employed here against the 'email' medium and the more generalized 'web' link can serve to degrade communications with distant end services. Integrity attacks can also be deployed even in the

M&S is forecasting, not prediction

M&S of human populations can be and frequently is reflective of population level measures and trends. It is tempting to extrapolate that since the modeled populations reflect empirical populations, that modeled agents will reflect real-life agents. This extrapolation, though tempting, is unwise in the extreme. Construct is an excellent tool for group level interactions, trends, and supplying data to network analytic methods. Construct is not the right tool to model individual agents' actions and reactions to their specific environments.

Fundamentally, this M&S as depicted in this dissertation is sufficient for forecasting results of meaningful use to organizational leaders. Construct-based M&S is not however appropriate to predict the actions and reactions of specific individuals.

Integration with staff section recommendations

While this effort, if used in an organization, can repeatability forecast operational impacts along multiple MoIs, it does not yet attempt to convert those impacts into units of measure used by the resource management teams (e.g., US dollars). The new measure uses the term ‘wastes’ that could very well be ‘spare capacity.’ Spare capacity itself has a carrying cost, a phenomena that economists and SCM researchers have been aware of for years. What neither the ABM simulation, nor simple spreadsheets can do is decide for the organizational leaders. These systems can provide data points, indications of probability, sensitivity analysis, and other forms of input to leaders—but fundamentally it is up to organizational leaders to decide how best to attain mission assurance within their given resource limits. It is also up to those leaders to perform expectation management for their higher headquarters or leaders as well—they are no less immune to profound disruption when their expectations of ‘return to normal’ are violated.

Contributions

There are six contributions from this dissertation to the field of computational modeling of organizations and to organizational resilience as a component of organizational science. The first three are applicable directly to the study of resilience and the last three are technology-centric contributions that support resilience assessments.

The first contribution is a brand-new static measure of assessment within the theoretical structure of Dynamic Network Analysis (DNA) (e.g., multimode and multi-link graphic analysis). This was the function of resilience relating needs, redundancy, and near isolation to a final value as [Equation 14](#) depicts. This measure builds on the traditions of organizational theory and resilience engineering, as well as supply chain management work by quantifying the interplay between spare capacity in knowledge and resources, as well as existing shortfalls and near single points of failure.

The second contribution is a rapid process to generate mission assurance models for specific organizations. This process is responsive to leaders’ perceptions of ‘now’ and not weeks or months ago. It is also responsive to forecasting scenarios to help plan future resource commitment. This rapid process is through the application of SNA and DNA to mission

assurance and resilience in contested cyber environments—unlike other state of the art cyber risk management techniques.

The third contribution is the incorporation of adaptive agents into mission assurance and resilience M&S. The majority of cyber risk management techniques do not incorporate the human element into organizational resilience M&S efforts. Supporting this contribution are the generalized assessments of resilience across multiple categorical and quantitative inputs of structure. Additionally, there are generalized assessments of resilience across multiple forms of contested cyber environments for baseline conditions and under mitigation efforts.

The three technology-centric contributions revolve around further refinements to the [D2M process](#) under development at CASOS as well numerous technical updates, major and minor modifications to the Construct ABM simulation. Some of the modifications derived from extensive refactoring of code written by a multitude of developers over the years. Some were integration of automated code documentation tools with the code base and the incorporation of inline commenting and source-code level documentation. One of the larger major modifications was the initial development and use of test cases integrating a unit test framework. The unit test addition to the code base increases confidence that the fundamental function of the system remains consistent across the versions and years. Regression testing is a key benefit of the unit test add-ons.

Another substantial technological addition to Construct was implementing task transactive memory—an error prone and cognitively modeled perception by egos of tasks assigned to their alters within a simulation environment. Task-based homophily is now a capability that modelers can use, or not, based on the nature of their research and questions of interest. By adding this capability, modelers who desire to incorporate similarity of assigned tasks into agent behavior can do so.

The last technology-oriented contribution is a DoD-specific thesaurus suitable for continued use, reuse, and expansion within the DoD for the D2M process. Thesauri can represent an enormous psychological barrier to use as well as a resource barrier; not all organizations can afford to create a thesaurus for use just by themselves. By using the thesaurus developed for this dissertation, future DoD organizations can increase their confidence in D2M generated models as well as speed of development of those models.

Insights and Surprises

An expected result of this dissertation is that there is substantial room for increased cooperation between research communities in organizational behavior and resilience, organizational design, and cyberspace operations and security!

Starting places

I started on the road to this dissertation with the complete and unquestioning conviction that military cyberspace operations could dramatically change the shape of future warfare. I had intended to use this work to demonstrate that manipulation of the right IT targets at the right time could render an organization incapable of functioning and much less militarily capable. To prove my intuition right, I thought I needed multiple and accessible models of adversaries' organization—unfortunately they are less prone to publishing in English the details of how they organize, train, and equipment in than we Americans. As a proof of concept, I decided to use the American DoD as my target, and its doctrine as the basis of the models I needed to attack and render helpless with a few judicious cyberspace operations.

What I have learned instead is that technology focused views of the world may not be adequate to forecast the future of cyberspace warfare. I'm a technologist by education and training, an Infantry officer by profession, military education, and training. I came to this realization because, excepting degenerate cases, creating scenarios and situations where dramatic effects were obvious has proven an elusive goal for the strategic and operational organizations I modeled

Nuance is necessary

There is no bumper sticker summation of this work that captures both the primary results and the caveats to those results. A non-discerning reader might miss that the military organizations I modeled generalize to some types of organizations, but certainly not all, and certainly not to IT dominated organizations (e.g., exchange traded funds ([ETF](#))), or manufacturing lines. By choosing to limit the research to small sub-sets of the organization, in particular the organizational leadership and operational planners, a reader may wrongly extrapolate that an entire organization is unaffected by the simulated effects in my virtual experiments. Recall from Figure 115 that human agent performance went up when IT agents were removed from the organization, while IT-agent performance went down as well as multiple

other IT-agent MoIs. Are these result inherently contradictory? It is an open question, but my intuition is they are consistent with reality for some organizations and not others.

Nuance and granularity are also appropriate in which sub-organizations to study. As discussed in the [Limitations and Future Work](#) section, it is foreseeable that there are attack scenarios that greatly impact one sub-group of an organization (e.g., coordinating air craft landing and takeoffs) while not impacting another (e.g., logistics resupply of fuel to the airport). Averaging across both groups can give an artificially sanguine picture to leadership, and extrapolating from a single good or horrid case can provoke Pollyanna or apocalyptic predictions. It is also foreseeable that some attacks effects may have effects not present in any of the measures I have discussed. A prime example of such an attack could be a complete loss of confidentiality to the HR sections databases about all of the organization's personnel. The psychological effects of such an event on sub-group and population MoI are not within the reach of the Construct M&S environment.

My top three surprises

Of all the surprises I encountered while conducting this research, I leave the reader with the top three. Each of these surprises have implications not only for future researchers in the field of cyber resilience, but also for organizational leaders. The three surprises are shown below:

- The modeled organizations were more resilient to cyber attacks than I predicted. I have spent a number of my professional Soldier years in joint strategic and operational headquarters as a staff officer. I had expected there would be ample and obvious evidence of the criticality of IT. I now recognize that I entered the research effort with an experiential bias toward the value of IT to everyone. I was aware that some portions of the organizations I worked at were more dependent than others, but I assumed significance throughout the organization. This research provides evidence that context of attacks, their timing, targeting, and second and third order effects contribute to variations in effects as well as perceived importance. It also provides evidence that human-dominated organizations, those with large reservoirs of tacit knowledge un-reachable by cyber attacks, are less likely to suffer ill effects of contested cyber environments.
- The modeled mitigations were not as obviously effective as I expected. Though all four were positively correlated with statistical significance to improvement during attacks, I had expected them to have, individually and combined, more obvious positive benefits. This surprise is tied to the first however—if the leadership is not as dependent on IT as I thought, the mitigations will not be as relevant to the leadership. It also contributes to my original justification for using M&S—real mitigations cost resources to put in place, and M&S may help identify those with a higher likelihood of efficacy.

- I had every intent of making the workflow first depicted in Figure 35 accessible to any DoD organization that cared to use M&S in its pursuit of cyber resilience. It is now my assessment that though this research is imminently repeatable, it requires more specialized knowledge and time than most DoD organizations will be willing to dedicate to its use. Further automation and process simplification is necessary before this approach could become widespread. Additionally, it would be very easy for casual users to misinterpret results, attribute causality over correlation, or otherwise use the M&S outputs in pursuit of agendas over simple mission assurance estimates.

Operational Implications

Below is a set of implications to operations based on the models I put under test and the results of the virtual experiments. The implications are both organization based, as well as leader based.

- When leaders hear the phrase “mission assurance” or “cyber resilience,” they should immediately ask: resilient to what, for whom, to what extent and to for what duration. This information will allow leaders to shape their expectations and prepare for adversity.
- Organizations with very little slack or spare capacity (for tasks, information flow, or other organizational missions) are brittle, the exact opposite of resilient. Spare capacity, resources permitting, can be human, IT, or combinations of both.
- Targeting matters, extrapolating resilience to targeted effects from the ability to cope with everyday IT problems is unsupported by evidence and probably not a good idea. Leaders should presume professional adversaries are trying to find the point(s) to target and cause the advantage(s) to their own their purposes.
- Integrity attacks and their effects are more pernicious than the others. The injection of moderately or completely wrong data into friendly decision cycles may be difficult to identify, and even more difficult to eradicate (urban legends several for years and decades).
- Expectation management matters. Resilient organizations communicate to their members both current information as well as realistic expectations for the future. Pollyanna predictions, when violated, cause greater negative effects than news of ‘it will take a long time’ to return to pre-event status.
- When leaders receive doom and gloom predictions of contested cyber environments, they should challenge themselves and their sub-groups to define quitting criteria. If they cannot picture or define how or why they would choose to quit their missions in a contested environment, they can start defining how they will adapt, and begin practicing the adaptation to make degradation smoother and not ad hoc.
- This methodology is a tool, suitable to some but not all organizations and scenario forecasting. This method is repeatable, supports exploration of good ideas’ efficacy without enormous resource commitment, and can inform leaders decisions for the kinds of models it supports. It does not currently support processes such as time-sensitive targeting or manufacturing. Don’t misapply tools to incorrect tasks.
- Subject Matter Experts for model review and construction is essential. SMEs for the models in this dissertation were able to see, very quickly and with little effort, holes in the groups and sub-groups of the modeled organizations. They were also able to rapidly point to additional documents that contained appropriate text, or point to the appropriate and small

selection of pictures and diagrams to transcribe into text for ingestion by the D2M process. Additionally, SMEs assist in establishing the first claims of face validity through their corrections and adjustments. They also assist in justifying omissions or inclusions of elements in the model that a research unfamiliar with the domain might otherwise miss.

- Information flow, task performance as accuracy, and other MoIs successfully used in these strategic and operational models may not be apropos for a tactical model. Tactical organizations, though also using information to control their operations, are the level of war tasked with planning and conducting battles, usually of limited duration and often in very time constrained environments. They have a tendency to emphasis action even in the face of insufficient information. Action-counter action cycles between friendly forces and adversaries is not a use case Construct currently supports.

Organizations are at their most fundamental level, collections of people, following sets of rules, procedures, and policies, supported and enabled by their equipment and tools. This area of research is rife with missed opportunities to bring researchers who specialize in people together with researchers who specialize in technology, and numerous other fields I discussed in the literature review. Resilience to contested cyber environments may be new, but resilience to adversity is something we humans have been doing for tens of thousands of years!

References

- 48 CFR Parts 202, 203, 211, et al. (2011).
- Abbott, R. P., Chin, J. S., Donnelley, J. E., Konigsford, W. L., Tokubo, S., & Webb, D. A. (1976). Security analysis and enhancements of computer operating systems: DTIC Document.
- Abreu, E. (2001, 9 May 2001). Cyberattack Reveals Cracks in the U.S. Defense. *PC World*.
- Akintoye, A. S., & MacLeod, M. J. (1997). Risk analysis and management in construction. *International Journal of Project Management*, 15(1), 31-38.
- Al-Bahar, J. F., & Crandall, K. C. (1990). Systematic risk management approach for construction projects. *Journal of Construction Engineering and Management*, 116(3), 533-546.
- Alberts, C. J., & Dorofee, A. J. (2010). Risk Management Framework (pp. 72). Pittsburgh, PA: Software Engineering Institute (SEI).
- Alexander, K. (2012). *Statement of General Keith B. Alexander, Commander, United States Cyber Command, before the Senate Committee on Armed Services*. Washington, DC: Department of Defense Retrieved from <http://www.armed-services.senate.gov/statemnt/2012/03%20March/Alexander%2003-27-12.pdf>.
- American National Standards Institute (ANSI), I. (2009). ASIS SPC.1-2009, Organizational Resilience Standard (Vol. ASIS SPC.1-2009, pp. 66). 1625 Prince Street, Alexandria, VA 22314-2818, USA: ASIS International.
- Andrijcic, E., & Horowitz, B. (2006). A Macro-Economic Framework for Evaluation of Cyber Security Risks Related to Protection of Intellectual Property. *Risk Analysis*, 26(4), 907-923. doi: 10.1111/j.1539-6924.2006.00787.x
- Argote, L. M., R. (2003). Transactive memory in dynamic organizations. In R. P. a. E. Mannix (Ed.), *Understanding the dynamic organization* (pp. 135-162). Mahwah, NJ: Lawrence Erlbaum Associates.
- Arthur, C. (2011). Gartner slashes 2011 PC sales forecast again as consumers stay wary. *Guardian.co.uk*. Retrieved from <http://www.guardian.co.uk/technology/2011/sep/08/gartner-pc-sales-forecast-slashed-2011>
- Ash, J. S., Berg, M., & Coiera, E. (2004). Some unintended consequences of information technology in health care: the nature of patient care information system-related errors. *Journal of the American Medical Informatics Association*, 11(2), 104-112. doi: 10.1197/jamia.M1471
- Ashmore, W. C. (2009). *Impact of Alleged Russian Cyber Attacks*. Fort Leavenworth, KS: Retrieved from <http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA504991>.
- Baker, D. P., Day, R., & Salas, E. (2006). Teamwork as an Essential Component of High-Reliability Organizations. *Health Services Research*, 41(4p2), 1576-1598. doi: 10.1111/j.1475-6773.2006.00566.x
- Baldwin, A., Picavet, F., & Reiners, J. (2009). Bridging the collaboration gap - Results from a global defense survey on collaboration during coalition operations. Somers, NY 10589: IBM Global Business Services.

- Bandyopadhyay, T., Mookerjee, V. S., & Rao, R. C. (2009). Why IT managers don't go for cyber-insurance products. *Communications of the ACM*, 52, 68-73.
- Barron, J. (2003). The Blackout of 2003: The Overview; Power surge blacks out northeast, hitting cities in 8 states and canada; midday shutdowns disrupt millions. *New York Times*. Retrieved from <http://www.nytimes.com/2003/08/15/nyregion/blackout-2003-overview-power-surge-blacks-northeast-hitting-cities-8-states.html?pagewanted=print&src=pm>
- Bartel, A. P. (1994). Productivity gains from the implementation of employee training programs. *Industrial relations: a journal of economy and society*, 33(4), 411-425. doi: 10.1111/j.1468-232X.1994.tb00349.x
- Bigrigg, M. W., Carley, K. M., Manousakis, K., & McAuley, A. (2009). *Routing Through an Integrated Social and communication Network*. Paper presented at the The 2009 Military Communications Conference (MILCOM'09), Boston, MA. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5379848&tag=1
- Bisbey, R., & Hollingsworth, D. (1978). Protection Analysis: Final Report (pp. 31). Marina del Rey, CA: Information Sciences Institute (ISI), USC.
- Bishop, M. (1995). A taxonomy of unix system and network vulnerabilities (D. o. C. Science, Trans.) (pp. 35): University of California at Davis.
- Bishop, M. (2003). What is computer security? *Security & Privacy, IEEE*, 1(1), 67-69. doi: 10.1109/MSECP.2003.1176998
- Bishop, M., Carvalho, M., Ford, R., & Mayron, L. M. (2011). *Resilience is more than availability*. Paper presented at the Proceedings of the 2011 workshop on New security paradigms workshop, Marin County, CA.
- Bishop, M., Engle, S., Peisert, S., Whalen, S., & Gates, C. (2009a). *Case studies of an insider framework*. Paper presented at the System Sciences, 2009. HICSS'09. 42nd Hawaii International Conference on.
- Bishop, M., Engle, S., Peisert, S., Whalen, S., & Gates, C. (2009b). *We have met the enemy and he is us*. Paper presented at the Proceedings of the 2008 workshop on New security paradigms.
- Blei, D. M., Ng, A. Y., & Jordan, M. I. (2003). Latent dirichlet allocation. *Journal of Machine Learning Research*, 3, 993-1022.
- Böhme, R. (2005). *Cyber-insurance revisited*. Paper presented at the Workshop on the Economics of Information Security (WEIS), Harvard University, Cambridge, MA.
- Böhme, R., & Kataria, G. (2006). *Models and measures for correlation in cyber-insurance*. Paper presented at the Workshop on the Economics of Information Security (WEIS), University of Cambridge, UK.
- Bonacich, P. (1972a). Factoring and weighting approaches to status scores and clique detection. *Journal of Mathematical Sociology*, 2, 113-120.
- Bonacich, P. (1972c). Technique for Analyzing Overlapping Memberships. In H. Costner (Ed.), *Sociological Methodology* (pp. 176-185). San Francisco: Jossey-Bass.
- Borgatti, S. P., Carley, K. M., & Krackhardt, D. M. (2006). Robustness of Centrality Measures under Uncertainty. *Social Networks*, 28(2), 124-136.
- Borshchev, A., & Filippov, A. (2004, July 25 - 29, 2004). *From system dynamics and discrete event to practical agent based modeling: reasons, techniques, tools*. Paper presented at the The 22nd International Conference of the System Dynamics Society, Oxford, England.

- Börzel, T., & Knoll, M. (2014). It's the Policy, Stupid! Sector-Specific Non-compliance in the European Union. *Sector-Specific Non-compliance in the European Union*.
- Box, G. E. P. (1979). All Models Are Wrong But Some Are Useful. In R. L. Launer & G. N. Wilkinson (Eds.), *Robustness in Statistics* (pp. 202). New York, NY: Academic Press.
- Box, G. E. P., & Behnken, D. (1960). Some new three level designs for the study of quantitative variables. *Technometrics*, 2(4), 455-475.
- Bozeman, B., & Feeney, M. K. (2011). *Rules and red tape: A prism for public administration theory and research*: ME Sharpe.
- Brown, D. G., Riolo, R., Robinson, D. T., North, M., & Rand, W. (2005). Spatial process and data models: Toward integration of agent-based models and GIS. *Journal of Geographical Systems*, 7(1), 25-47. doi: 10.1007/s10109-005-0148-5
- Bumiller, E., & Shanker, T. (2012). Panetta Warns of Dire Threat of Cyberattack on the U.S. *The New York Times*. Retrieved from The New York Times website: <http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html?pagewanted=all&pagewanted=print>
- Cameron, K. (1986). A study of organizational effectiveness and its predictors. *Management Science*, 32(1), 87-112.
- Canessa, E., & Riolo, R. L. (2003). The Effect of Organizational Communication Media on Organizational Culture and Performance: An Agent-Based Simulation Model. *Computational & Mathematical Organization Theory*, 9(2), 147-176. doi: 10.1023/b:cmot.0000022753.91962.99
- Carew, S. (2012). Hurricane Sandy disrupts Northeast US telecom networks. *Reuters News wire*. Retrieved from <http://www.reuters.com/assets/print?aid=USL1E8LU30X20121030>
- Carley, K. M. (1986). An Approach for Relating Social Structure to Cognitive Structure. *Journal of Mathematical Sociology*, 12(2), 137-189. doi: 10.1080/0022250X.1986.9990010
- Carley, K. M. (1991). Designing Organizational Structures to Cope with Communication Breakdowns: A Simulation Model. *Industrial Crisis Quarterly*, 5, 19-57. doi: 10.1177/108602669100500102
- Carley, K. M. (1992). Organizational Learning and Personnel Turnover. *Organization Science*, 3(1), 20-46. doi: 10.1287/orsc.3.1.20
- Carley, K. M. (1994). Extracting Culture through Textual Analysis. *Poetics*, 22, 291-312. doi: 10.1016/0304-422X(94)90011-6
- Carley, K. M. (1995). Communication Technologies and Their Effect on Cultural Homogeneity, Consensus, and the Diffusion of New Ideas. *Sociological Perspectives*, 38(4), 547-571. doi: 10.2307/1389272
- Carley, K. M. (2002a). Smart agents and organizations of the future. In L. Lievrouw, and Sonia Livingstone (Ed.), *The Handbook of New Media* (pp. Chapter 12, 205-220). Thousand Oaks, CA: Sage.
- Carley, K. M. (2002d). Summary of Key Network Measures for Characterizing Organizational Architectures. *Unpublished document*.
- Carley, K. M. (2003). Dynamic Network Analysis. In R. Breiger, K. M. Carley, & P. Pattison (Eds.), *Dynamic Social Network Modeling and Analysis: Workshop Summary and Papers, Committee on Human Factors, National Research Council* (pp. 133-145). Washington, DC: National Research Council.

- Carley, K. M. (2011). *Lesson 2 - Key Entities and Basic Measures - SNA*. Dynamic Network Analysis Course Lecture Slides. Institute of Software Research. Carnegie Mellon University. Pittsburgh, PA.
- Carley, K. M., Bigrigg, M. W., Papageorgiou, C., Johnson, J., Kunkel, F., Lanham, M. J., . . . Van Holt, T. (2011). *Rapid Ethnographic Assessment: Data-To-Model*. Paper presented at the Human Social Culture and Behavioral Modeling (HSCB) Focus 2011: Integrating Social Science Theory and Analytic Methods for Operational Use, Chantilly, Virginia, USA.
- Carley, K. M., Columbus, D., Bigrigg, M. W., Diesner, J., & Kunkel, F. (2011). AutoMap User's Guide 2011 (Center for the Computational Analysis of Social and Organizational Systems (CASOS), Trans.) [Technical report] / Carnegie Mellon University, School of Computer Science, Institute for Software Research. Pittsburgh, PA: Carnegie Mellon University.
- Carley, K. M., Joseph, K., Lanham, M. J., Morgan, G. P., & Kowalchuck, M. (2014). Construct User Guide (Center for the Computational Analysis of Social and Organizational Systems (CASOS), Trans.) [Technical report] / Carnegie Mellon University, School of Computer Science, Institute for Software Research (pp. 125). Pittsburgh, PA: Carnegie Mellon University.
- Carley, K. M., & Kaufer, D. (1993). Semantic Connectivity: An Approach for Analyzing Semantic Networks. *Communication Theory*, 3(3), 183-213.
- Carley, K. M., & Kim, E. J. (2008). *Random Graph Standard Network Metrics Distributions in ORA* [Technical report] / Carnegie Mellon University School of Computer Science Institute for Software Research International CMU-ISR-08-103 Retrieved from <http://www.casos.cs.cmu.edu/publications/papers/CMU-ISR-08-103.pdf>
- Carley, K. M., & Krackhardt, D. (1999, June). *A Typology for C2 Measures*. Paper presented at the Proceedings of the 1999 International Symposium on Command and Control Research and Technology, Newport, RI.
- Carley, K. M., & Lanham, M. J. (2012). A Complex Socio-Technical System Perspective of Resilient Command & Control (C2) (Key Note Address). *Computational CyberSecurity in Compromised Environments (C3E) Workshop* [Powerpoint Slides]. West Point, NY: Office of the Director of National Intelligence (ODNI) & National Security Agency (NSA).
- Carley, K. M., & Lee, J.-S. (1998). Dynamic Organizations: Organizational Adaptation in a Changing Environment. In J. Baum (Ed.), *Advanced in Strategic Management, Roots of Strategic Management Research* (Vol. 15, pp. 269-297). Greenwich, CT: JAI Press.
- Carley, K. M., Morgan, G. P., Lanham, M. J., & Pfeffer, J. (2012, 21-25 July). *Multi-Modeling and Socio-cultural complexity: Reuse and Validation*. Paper presented at the 2nd International Conference on Cross-Cultural Decision Making, San Francisco, CA.
- Carley, K. M., Morgan, G. P., Lanham, M. J., & Pfeffer, J. (2012). Multi-Modeling and Sociocultural Complexity. In D. D. Schmorow & D. M. Nicholson (Eds.), *Advances in Design for Cross-Cultural Activities Part II* (Vol. 2, pp. 128-137): RC Press.
- Carley, K. M., & Pfeffer, J. (2012a). *Concepts and Measures for Two-Mode and Multi-Mode Networks Poster*. Institute of Software Research (ISR), Center for Computational Analysis of Social and Organizational Systems (CASOS). Carnegie Mellon University. Pittsburgh, PA.

- Carley, K. M., & Pfeffer, J. (2012c). *Two-Mode and Multi-Mode Networks*. Institute of Software Research. Pittsburgh, PA.
- Carley, K. M., Pfeffer, J., Reminga, J., Storrick, J., & Columbus, D. (2012). ORA User's Guide 2012 (Center for the Computational Analysis of Social and Organizational Systems (CASOS), Trans.) [Technical report] / Carnegie Mellon University, School of Computer Science, Institute for Software Research. Pittsburgh, PA: Carnegie Mellon University.
- Cashell, B., Jackson, W. D., Jickling, M., & Webel, B. (2004). The economic impact of cyber-attacks *CRS Report for Congress*. Washington, D.C.: Congressional Research Service, Library of Congress.
- Cataldo, M., Herbsleb, J. D., & Carley, K. M. (2008). *Socio-technical congruence: a framework for assessing the impact of technical and work dependencies on software development productivity*. Paper presented at the Proceedings of the Second ACM-IEEE international symposium on Empirical software engineering and measurement, Kaiserslautern, Germany. <http://dl.acm.org/citation.cfm?id=1414008>
- CBS/AP. (2012a). Power outages on Long Island spur lawsuits and punches in Sandy's wake. *CBSNews*. Retrieved from CBSNews website: http://www.cbsnews.com/8301-201_162-57549158/power-outages-on-long-island-spur-lawsuits-and-punches-in-sandys-wake/
- CBS/AP. (2012c). Superstorm Sandy: More than 7 million without power. *CBSNews*. Retrieved from CBSNews Hurricane Sandy website: http://www.cbsnews.com/8301-201_162-57542015/superstorm-sandy-more-than-7-million-without-power/
- Chapman, I. M., Leblanc, S. P., & Partington, A. (2011). *Taxonomy of cyber attacks and simulation of their effects*. Paper presented at the Proceedings of the 2011 Military Modeling & Simulation Symposium, Boston, Massachusetts. <http://dl.acm.org/citation.cfm?id=2048569>
- Christensen, C. M. (2006). The Ongoing Process of Building a Theory of Disruption. *Journal of Product Innovation Management*, 23(1), 39-55. doi: 10.1111/j.1540-5885.2005.00180.x
- Chubb Group of Insurance Companies. (2012). Chubb Public Company Risk Survey: Cyber. Retrieved 16 December 2012, 2012, from <http://www.chubb.com/infographics/chubb3/index.html>
- Clark, W. K., & Levin, P. L. (2009). Securing the Information Highway. *Foreign Affairs*, 88(6), 8.
- CNSS. (2010). (CNSSI) National Information Assurance (IA) Glossary (U) (Vol. CNSSI-4009). Ft Meade, MD: Committee on National Security Systems (CNSS) Secretariat, NSA.
- Cohen, D. R., & Anderson, R. D. (2000). Insurance Coverage for Cyber-Losses. *Tort & Insurance Law Journal*, 35(4), 891-927.
- Cohen, F. (1999). Simulating cyber attacks, defences, and consequences. *Computers & Security*, 18(6), 479-518.
- Comfort, L. K. (2006). Risk and Resilience: Inter-organizational Learning Following the Northridge Earthquake of 17 January 1994. *Journal of Contingencies and Crisis Management*, 2(3), 157-170.
- Computing with HTCondor. (2015, 8 April 2015). Retrieved 12 April, 2015, from <http://research.cs.wisc.edu/htcondor/>
- Conrath, D. W. (1973). Communications Environment and Its Relationship to Organizational Structure. *Management Science*, 20(4), 586-603.
- contested. (2013). Merriam-Webster. Retrieved 9 January, 2013, from <http://www.merriam-webster.com/dictionary/contested>

- Cooper, M. C., Lambert, D. M., & Pagh, J. D. (1997). Supply chain management: more than a new name for logistics. *International Journal of Logistics Management*, 8(1), 1-14. doi: 10.1108/09574099710805556
- Coping with Catastrophe: Building an Emergency Management System to Meet People's Needs in Natural and Mammade Disasters*. (1993). Washington: National Academy of Public Administration.
- Coutu, D. L. (2002). How resilience works. *Harvard Business Review*, 80(5), 46-50.
- Crichton, M. T., Ramsay, C. G., & Kelly, T. (2009). Enhancing Organizational Resilience Through Emergency Planning: Learnings from Cross-Sectoral Lessons. *Journal of Contingencies and Crisis Management*, 17(1), 24-37. doi: 10.1111/j.1468-5973.2009.00556.x
- Cyert, R. M., & March, J. G. (1963). *Behavioral Theory of the Firm*. Englewood Cliffs, NJ: Prentice-Hall.
- Damanpour, F. (1991). Organizational Innovation: A Meta-Analysis of Effects of Determinants and Moderators. *The Academy of Management Journal*, 34(3), 555-590. doi: 10.2307/256406
- Danial, A. (2015). cloc: Count Lines of Code (Version 1.62) [Perl]. sourceforge.net. Retrieved from <http://cloc.sourceforge.net/>
- Davis, J. (2007). Hackers take down the most wired country in europe. *Wired Magazine*, 15(9), 15-09.
- Davis, P. K. (2006). Effects-Based Operations - A Grand Challenge for the Analytical Community (pp. 117). Arlington, VA.
- Dawes, B., Abrahams, D., Josuttis, N. M., & Et. al. Boost Getting Started. Retrieved November, 2014, from http://www.boost.org/doc/libs/1_57_0/more/getting_started/index.html
- Defense Business Board. (2010). A Review of Spectrum Management.
- Information Assurance (DoD Instruction 8500.01E) (2007).
- DHS. (2011). *Enabling Distributed Security in Cyberspace - Building a Healthy and Resilient Cyber Ecosystem with Automated Collective Action*. Washington, DC: Retrieved from <http://www.dhs.gov/xlibrary/assets/nppd-cyber-ecosystem-white-paper-03-23-2011.pdf>.
- Diesner, J., & Carley, K. M. (2004, June 27-29, 2004). *Using Network Text Analysis to Detect the Organizational Structure of Covert Networks*. Paper presented at the North American Association for Computational Social and Organizational Science (NAACSOS) Conference, Pittsburgh, PA.
- Diesner, J., & Carley, K. M. (2005). Revealing social structure from texts: Meta-Matrix text analysis as a novel method for network text analysis. In V. K. Narayanan & D. J. Armstrong (Eds.), *Causal Mapping for Information Systems and Technology Research: Approaches, Advances, and Illustrations* (pp. 81-108). Harrisburg, PA: Idea Group Publishing.
- Diesner, J., & Carley, K. M. (2011). Words and Networks. In G. Barnett & J. G. Golson (Eds.), *Encyclopedia of Social Networking* (pp. 958-961): Sage.
- Dolev, D., & Yao, A. C. (1983). On the security of public key protocols. *IEEE Transactions on Information Theory*, 29(2), 198-208.
- Dutton, J. E., & Dukerich, J. M. (1991). Keeping an eye on the mirror: Image and Identity in organizational adaptation. *The Academy of Management Journal*, 34(3), 517-554.
- Economist Editorial. (2012). Cyber-warfare - Hype and fear. *The Economist*.

- Effken, J. A., Brewer, B. B., Patil, A., Lamb, Gerri S., Verran, J. A., & Carley, K. M. (2005). Using OrgAhead, a computational modeling program, to improve patient care unit safety and quality outcomes. *International Journal of Medical Informatics*, 74, 7-8. doi: 10.1016/j.ijmedinf.2005.02.003
- Ekstrom, J. A., & Lau, G. T. (2008). *Exploratory text mining of ocean law to measure overlapping agency and jurisdictional authority*. Paper presented at the International Conference on Digital Government Research, Montreal, Canada.
- Elder, R. J. (2008). *Global Operations and Mission Assurance in a Contested Cyber Environment*. Paper presented at the The 2008 GTISC Security Summit - Emerging Cyber Security Threats, Georgia Institute of Technology.
<http://smartech.gatech.edu/bitstream/handle/1853/26300/presentation.pdf?sequence=2>
- Elder, R. J., & Levis, A. H. (2010). *Use of Multi-Modeling to Inform Cyber Deterrence Policy and Strategies*. Paper presented at the Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy, Washington, D.C.
http://sysarch.gmu.edu/main/media/publications/docs/Elder_NRC_Cyberdeterrence.pdf
- Emery, J. D. (2002). Designing Firm Integrating Processes from the Knowledge-Based View—Graduate Student Best Paper Award, CASOS 2002 Conference. *Computational & Mathematical Organization Theory*, 8(3), 243-250.
- ePM. (2012). ePM Technology. Retrieved 20 December, 2012, from
<http://www.epm.cc/technology.php#SimVision>
- Federal Information Security Management Act (FISMA), Pub. L. No. 107-347 § Subchapter III, Chapter 35 Title 44 USC 16 (NIST 2002 2002).
- Festinger, L. (1950). Informal Social Communication. *Psychological Review*, 57, 271-282.
- Festinger, L. (1954). A theory of social comparison processes. *Human Relations*, 7, 117-140.
- Flinn, S., & Stoyles, S. (2005). *Omnivore: risk management through bidirectional transparency*. Paper presented at the Proceedings of the 2004 workshop on New security paradigms, Nova Scotia, Canada.
- Frankel, Y., Gemmell, P., Mackenzie, P. D., & Yung, M. (1997, 20-22 October). *Optimal-resilience proactive public-key cryptosystems*. Paper presented at the 38th Annual Symposium on Foundations of Computer Science.
- Frantz, T. L., & Carley, K. M. (2005). Relating Network Topology to the Robustness of Centrality Measures (I. o. S. R. I. School of Computer Science (SCS), Center for the Computational Analysis of Social and Organizational Systems (CASOS), Trans.). Pittsburgh: Institute of Software Research, School of Computer Science, Carnegie Mellon University.
- Frantz, T. L., & Carley, K. M. (2007). *The Impact of Knowledge Misrepresentation on Organization Performance Dynamics*. Paper presented at the North American Association for Computational Social and Organizational Sciences, Atlanta, GA.
- Freeman, L. C. (1977). A Set of Measures of Centrality Based on Betweenness. *Sociometry*, 40, 35-41.
- Freeman, L. C. (1979). Centrality in social networks I: Conceptual clarification. *Social Networks*(1), 215-239.
- Freeman, L. C., Roeder, D., & Mullholland, R. (1979). Centrality in social networks: II. Experimental Results. *Social Networks*, 2, 119-141.
- Galvin, D., Giles, L., & Stade, G. (Eds.). (2003). *Sun Tzu: The Art of War*. New York: Barnes and Noble Classics.

- Gilpin, D. (2008). Does virtualisation equal resilience? *ITadviser*, Winter, 3.
- Gligor, V. D. (2005). *Guaranteeing access in spite of distributed service-flooding attacks*. Paper presented at the Security Protocols.
- Gligor, V. D. (2008). The Fragility of Adversary Definitions in Cryptographic Protocols. *DCS Lecture Series*. New Brunswick, NJ: Rutgers University.
- Gloor, P. A., & Zhao, Y. (2006). *Analyzing actors and their discussion topics by semantic social network analysis*. Paper presented at the The 10th IEEE International Conference on Information Visualisation, London, UK.
http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1648252&tag=1
- Goldman, H., Klopott, F., & Vekshin, A. (2012). NYC Commuter Week Faces Uncharted Ground as Storm Brews. *Bloomberg, LP*. Retrieved from:
<http://www.bloomberg.com/news/print/2012-11-04/new-york-commuters-to-begin-week-navigating-uncharted-territory.html>
- Gorman, S., Cole, A., & Dreazen, Y. (2009). Computer Spies Breach Fighter-Jet Project. *Wall Street Journal*. Retrieved from
<http://online.wsj.com/article/SB124027491029837401.html#printMode>
- Graham, J. M. (2005). *Dynamic Network Analysis of the Network-Centric Organization: Towards an Understanding of Cognition & Performance*. (Doctor of Philosophy), Carnegie Mellon University, Pittsburgh. Retrieved from
<http://www.casos.cs.cmu.edu/publications/papers/CognitionAndPerformance.pdf>
- Graham, J. M., Schneider, M., Bauer, A., & Bessiere, K. G., C. (2004). *Shared Mental Models in Military Command and Control Organizations: Effect of Social Network Distance*. Paper presented at the 47th Annual Meeting of the Human Factors and Ergonomics Society, California.
- Grimaila, M. R., Mills, R. F., & Fortson, L. W. (2013). ***Improving the Cyber Incident Mission Impact Assessment (CIMIA) Process***. Paper presented at the 8th Cyber Security and Information Intelligence Research Workshop CSIIRW '08, Oak Ridge National Laboratory.
- Guilford, N. (2010). *Lessons Learned from Hurricane Katrina: Louisiana's Perspective on Emergency Management*. Paper presented at the Government Leadership and Management.
<http://www.nga.org/files/live/sites/NGA/files/pdf/OMCTLESSONSKATRINA.PDF>
- Gunderson, L. H. (2003). *Adaptive dancing: interactions between social resilience and ecological crises*: Cambridge University Press.
- Hamel, G., & Välikangas, L. (2003). The quest for resilience. *Harvard Business Review*, 81(9), 52-65.
- Hansman, S., & Hunt, R. (2005). A taxonomy of network and computer attacks. *Computers & Security*, 24(1), 31-43.
- Hartley, R., & Barnden, J. (1997). Semantic networks: visualizations of knowledge. *Trends in Cognitive Sciences*, 1, 169-175.
- Haythornthwaite, C. (2005). Social networks and Internet connectivity effects. *Information, Community & Society*, 8(2), 125-147.
- Headquarters Department of the Army. (2010). *Operational Terms and Graphics*. Washington, D.C.: Government Printing Office Retrieved from
http://armypubs.army.mil/doctrine/DR_pubs/dr_a/pdf/fm1_02.pdf.

- Hirshman, B., St. Charles, J., & Carley, K. M. (2011). Leaving us in tiers: can homophily be used to generate tiering effects? *Computation and Mathematical Organization Theory*, 17(4), 318-343. doi: 10.1007/s10588-011-9088-4
- Hirshman, B. R., Kowalchuck, M. J., & Carley, K. M. (2008). Modeling Information Access in Construct. Pittsburgh, PA: Carnegie Mellon University.
- Holling, C. S. (1973). Resilience and stability of ecological systems. *Annual review of ecology and systematics*, 1-23.
- Hollnagel, E., Woods, D. D., & Leveson, N. (Eds.). (2006). *Resilience Engineering (Ebk) Concepts and Precepts*. Hampshire, England: Ashgate Publishing.
- Hommes, C. H. (2001). Financial markets as nonlinear adaptive evolutionary systems.
- Hoo, K. J. S. H. (2000). *How much is enough? A risk management approach to computer security*: Stanford University.
- Horning, J. (2009). Words Matter: Privacy, Security, and Related Terms. In C. Gal, P. Kantor, & M. Lesk (Eds.), *Protecting Persons While Protecting the People* (Vol. 5661, pp. 57-62): Springer Berlin / Heidelberg.
- Howard, J. D. (1997). *An analysis of security incidents on the Internet 1989-1995*. (PhD), Carnegie Mellon University. Retrieved from <http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA389085> (ADA389085)
- Huber, G. P. (1991). Organizational Learning: The Contributing Processes and the Literatures. *Organization Science*, 2(1), 88-115. doi: 10.1287/orsc.2.1.88
- IBM. (2007). Frequently Asked Questions: IBM.
- Joint Staff J3. (2006). *Information Operations*. Washington, D.C.: Joint Staff Retrieved from http://www.dtic.mil/doctrine/new_pubs/jp6_0.pdf.
- Information Assurance (IA) and Support to Computer Network Defense (CND), 6510.01F C.F.R. (2011).
- Joint Staff J7. (2010a). *Department of Defense Dictionary of Military and Associated Terms*. Washington, D.C.: Joint Staff Retrieved from http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf.
- Joint Staff J7. (2010j). *Joint Operations*. Washington, D.C.: Joint Staff Retrieved from http://www.dtic.mil/doctrine/new_pubs/jp3_0.pdf.
- Joseph, K., Morgan, G. P., Martin, M. K., & Carley, K. M. (2013). On the Coevolution of Stereotype, Culture, and Social Relationships: An Agent-Based Model. *Social Science Computer Review*. doi: 10.1177/0894439313511388
- Jüttner, U., Peck, H., & Christopher, M. (2003). Supply chain risk management: outlining an agenda for future research. *International Journal of Logistics: Research and Applications*, 6(4), 197-210. doi: 10.1080/13675560310001627016
- Kaminski, P., Gosler, J. R., & Von Thuer, L. (2013). Resilient Military Systems and the Advanced Cyber Threat (U. AT&L, Trans.) (pp. 146). Washington, D.C.: Department of Defense.
- Kan, S. A. (2006). China: Suspected Acquisition of US Nuclear Weapon Secrets *CRS Report for Congress*. Washington, D.C.: DTIC.
- Kim, S. (2012). Stocks Rise as Markets Open After Hurricane Sandy. Retrieved 20 December 2012, 2012, from <http://abcnews.go.com/blogs/business/2012/10/stocks-rise-as-markets-open-after-hurricane-sandy/>
- Kleinberg, J. (1999). Authoritative sources in a hyperlinked environment. *Journal of the ACM*, 46(5), 604-632.

- Krackhardt, D., & Carley, K. M. (1998). *A PCANS Model of Structure in Organizations*. Paper presented at the International Symposium on Command and Control Research and Technology, Monterey, CA, USA.
- La Porte, T. R., & Consolini, P. M. (1991). Working in practice but not in theory: Theoretical challenge of high reliability organizations. *Journal of Public Administration Research and Theory*, 1(1), 19-47.
- Lally, L. (2013, 5-7 April). *Information Technology and Crisis Compliance: Implications for Studying Hurricane Sandy*. Paper presented at the Northeast Decision Sciences Institute Annual Meeting, New York, New York.
- Landwehr, C. E., Bull, A. R., McDermott, J. P., & Choi, W. S. (1994). A taxonomy of computer program security flaws. *ACM Computing Surveys (CSUR)*, 26(3), 211-254. doi: 10.1145/185403.185412
- Lanham, M. J. (2012a, October). Operating on Unconventional Terrain. *Army Communicator*, 37, 7-13.
- Lanham, M. J. (2012c, December). When the network dies. *Armed Forces Journal*, 10-13, 32.
- Lanham, M. J., Morgan, G. P., & Carley, K. M. (2011a, June). *Data-Driven Diffusion Modeling to examine Deterrence*. Paper presented at the IEEE Network Science Workshop, West Point, NY.
- Lanham, M. J., Morgan, G. P., & Carley, K. M. (2011b). Simulating Integrated Resilient Command and Control (C2) in Contested Cyber Environments (S. A. Laboratory, Trans.). In A. Levis, K. M. Carley, & G. Karsai (Eds.), *Resilient Architectures for Integrated Command and Control in a Contested Cyber Environment* (pp. 95-106). Fairfax, VA: The Volgenau School of Engineering Dept. of Electrical and Computer Engineering System Architectures Laboratory, George Mason University. Retrieved from <http://www.casos.cs.cmu.edu/publications/papers/2011SimulatingIntegratedResilientCommand.pdf>.
- Lanham, M. J., Morgan, G. P., & Carley, K. M. (2011e). Social Network Modeling and Simulation of Integrated Resilient Command and Control in Contested Cyber Environments (S. A. Laboratory, Trans.). In A. Levis, K. M. Carley, & G. Karsai (Eds.), *Resilient Architectures for Integrated Command and Control in a Contested Cyber Environment* (pp. 63-94). Fairfax, VA: The Volgenau School of Engineering Dept. of Electrical and Computer Engineering System Architectures Laboratory, George Mason University. Retrieved from <http://www.casos.cs.cmu.edu/publications/papers/2011SimulatingIntegratedResilientCommand.pdf>.
- Lanham, M. J., Morgan, G. P., & Carley, K. M. (2012). *Social Network Modeling and Simulation of Integrated Resilient Command and Control (C2) in Contested Cyber Environments*. Paper presented at the Sunbelt XXXIII, Redondo Beach, CA. http://www.insna.org/PDF/Sunbelt/32_AbstractPDF.pdf
- Lanham, M. J., Morgan, G. P., & Carley, K. M. (2014). Social Network Modeling and Agent-Based Simulation in Support of Crisis De-escalation. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 44(1), 103-110. doi: 10.1109/TSMCC.2012.2230255
- Lanham, M. J., Morgan, G. P., Carley, K. M., & Levis, A. (2011). *Multimodel Modeling In Support Of Crisis Deescalation*. Paper presented at the Sunbelt, St. Petersburg Beach, FL. http://www.insna.org/PDF/Sunbelt/31_AbstractPDF.pdf

http://alliance2.casos.cs.cmu.edu/project/Lists/Publication%20Tracking/Attachments/100/DNA_COA_Development.pptx

- Laundauer, T., Foltz, P., & Laham, D. (1998). An Introduction to Latent Semantic Analysis. *Discourse Processes*, 25, 259-284.
- Leblanc, S. P., Partington, A., Chapman, I., & Bernier, M. (2011). *An overview of cyber attack and computer network operations simulation*. Paper presented at the Proceedings of the 2011 Military Modeling & Simulation Symposium, Boston, Massachusetts.
<http://dl.acm.org/citation.cfm?id=2048572>
- Lee, J.-S., & Carley, K. M. (2004). OrgAhead: A Computational Model of Organizational Learning and Decision Making [Version2.1.5] (I. o. S. R. I. School of Computer Science (SCS), Center for the Computational Analysis of Social and Organizational Systems (CASOS), Trans.). Pittsburgh: Carnegie Mellon University.
- Lennon, M. (2011). Massive Series of Cyber Attacks Targeting 70+ Global Organizations Uncovered. *SecurityWeek*.
- Levine, J. M., Moreland, R. L., Argote, L., & Carley, K. M. (2005). Personnel Turnover and Team Performance (pp. 59). Pittsburgh, PA: University of Pittsburgh.
- Levis, A. H., Carley, K. M., & Karsai, G. (2011). *Resilient Architectures for Integrated Command and Control in a Contested Cyber Environment AFRL Report: SAL/FR-11-02* (pp. 169). Retrieved from
<http://www.casos.cs.cmu.edu/publications/papers/2011SimulatingIntegratedResilientCommand.pdf>
- Levis, A. H., & Perdu, D. M. (1996, September). *CAESAR II: A System for the Design and Evaluation of Command and Control Organizations*. Paper presented at the Proc. 2nd International Command and Control Research and Technology Symposium, Market Bosworth, England.
- Levitt, B., & March, J. G. (1988). Organizational Learning. *Annual Review of Sociology*, 14, 319-340.
- Levitt, R. E., & Kunz, J. C. Design your Project Organization as Engineers Design Bridges *CIFE Working Paper* (pp. 21): Stanford University.
- Lewis, J. A. (2005). Computer Espionage, Titan Rain and China. Retrieved from:
http://csis.org/files/media/csis/pubs/051214_china_titan_rain.pdf
- Lewis, J. A. (2010). The Cyber War Has Not Begun. Retrieved from Center for Strategic and International Studies Publications website: <http://csis.org/publication/cyber-war-has-not-begun>
- Lin, Z., & Carley, K. M. (1997). Organizational decision making and error in a dynamic task environment. *Journal of Mathematical Sociology*, 22(2), 125-149. doi: 10.1080/0022250X.1997.9990198
- Lochin, E., Pérennou, T., & Dairaine, L. (2012). When should I use network emulation? *Annals of Telecommunications*, 67(5), 247-255. doi: 10.1007/s12243-011-0268-5
- Louie, M. A., Carley, K. M., Haghsheenas, L., Kunz, J. C., & Levitt, R. E. (2003, 22-25 June). *Model Comparisons: Docking ORGAHEAD and SimVision (2003)*. Paper presented at the North American Association for Computational Social and Organizational Science (NAACSOS) Conference, Pittsburgh, Pa.
- Loveland, G., & Lobel, M. (2012). Cybersecurity: The new business priority. *View*, 15, 24-33.
- Low, B., Ostrom, E., Simon, C., & Wilson, J. (2003). Redundancy and diversity: do they influence optimal management. In F. Berkes, J. Colding, & C. Folke (Eds.), *Navigating*

- social-ecological systems: building resilience for complexity and change* (pp. 83-114). Cambridge, UK: Cambridge University Press.
- Lynn, W. J. I. (2010). Defending a New Domain. *Foreign Affairs*, 89(5), 97-108.
- Madni, A. M., & Jackson, S. (2009a). Towards a conceptual framework for resilience engineering *Systems Journal, IEEE* (Vol. 3, pp. 181-191).
- Madni, A. M., & Jackson, S. (2009c). Towards a conceptual framework for resilience engineering. *Systems Journal, IEEE*, 3(2), 181-191.
- March, J. G. (1991). Exploration and Exploitation in Organizational Learning. *Organizational Science*, 2(1), 71-87.
- March, J. G., & Olsen, J. (1975). The Uncertainty of the Past: Organizational Learning Under Ambiguity. *European Journal of Political Research*, 3, 147-171.
- Markose, S. M. (2005). Computability and Evolutionary Complexity: Markets as Complex Adaptive Systems (CAS)*. *The Economic Journal*, 115(504), F159-F192. doi: 10.1111/j.1468-0297.2005.01000.x
- Martin, M. K., Morgan, G. P., Joseph, K., & Carley, K. M. (2010). Impact of Information Loss and Information Error on Network-enabled Decision-making (pp. 29): DTIC.
- Masi, D. M. B., Smith, E. E., & Fischer, M. J. (2010). Understanding and mitigating catastrophic disruption and attack. *Sigma: Rare Events*, 10(1), 16-22.
- MathJax Consortium. (2014). MathJax Documentation. Retrieved November, 2014, from <http://www.mathjax.org/>
- McCoy, K. (2012, 5 November). New York commuters experience long lines. *USAToday*. Retrieved from <http://www.usatoday.com/story/news/nation/2012/11/04/new-york-superstorm-sandy/1680637/>
- McCulloh, I. (2009). *Detecting Changes in a Dynamic Social Network*. (Doctorate of Philosophy PhD), Carnegie Mellon University, Pittsburgh, PA. Retrieved from <http://www.casos.cs.cmu.edu/publications/papers/CMU-ISR-09-104.pdf> (CMU-ISR-09-104)
- McCulloh, I., & Carley, K. M. (2008). Dynamic Network Change Detection. *Proceedings of the 26th Army Science Conference. US ...*
- McCulloh, I., Daimler, Eric., & Carley, K. M. (2008, July 14-17, 2008). *Using Latent Semantic Analysis of Email to Detect Change in Social Groups*. Paper presented at the 2008 International Conference on Data Mining (DMIN 2008), Las Vegas, NV.
- McPherson, J. M., & Smith-Lovin, L. (1987). Homophily in Voluntary Organizations: Status Distance and the Composition of Face-to-Face Groups. *American Sociological Review*, 52, 370-379.
- McPherson, M., Lovin, L., & Cook, J. (2001). Birds of a Feather: Homophily in Social Networks. *Annual Review of Sociology*, 27(1), 415-444. doi: citeulike-article-id:3022278
- Mead, G. H. (1925). The genesis of the self and social control. *International Journal of Ethics*, 35(3), 251-277.
- Mergel, I., Diesner, J., & Carley, K. M. (2010). *Attention Networks among Members of Congress*. Paper presented at the XXX International Sunbelt Social Network Conference, Riva del Garda, Italy. http://www.andrew.cmu.edu/user/jdiesner/publications/mergel_diesner_carley_sunbelt_2010.html

- Merton, R. K. (1957, 1968). Continuities in the theory of reference groups and social structure. In M. R. K. (Ed.), *Social Theory and Social Structure* (pp. 281-386). New York, NY: Free Press.
- Meuer, H., Strohmaier, E., Dongarra, J., & Simon, H. (2012). <http://www.top500.org/statistics/overtime/>. In Top500_Nov2012 (Ed.), *Chrome & Screen Capture* (Vol. 612 x 627 px, pp. Screen Capture of a dynamic figure depicting the per-continent share of installed super computers as of November 2012). Fliederstr. 2, D-74915 Waibstadt-Daisbach, Germany: Prometheus GmbH.
- Meuer, H., Strohmaier, E., Simon, H., & Dongarra, J. (2012). Oak	Ridge Claims No. 1 Position on Latest TOP50 List with Titan, Press Release. In s.top500.org (Ed.), (pp. 2). University	of Mannheim,.
- Miller, J. H., & Moser, S. (2004). Communication and coordination. *Complexity*, 9(5), 31-40.
- Miller, J. H., & Page, S. E. (2007). *Complex Adaptive Systems - An Introduction to Computational Models of Social Life*. Princeton, NJ: Princeton University Press.
- Miller, K. D. (1992). A Framework for Integrated Risk Management in International Business. *Journal of International Business Studies*, 23(2), 311-331. doi: 10.2307/154903
- Min, H., & Zhou, G. (2002). Supply chain modeling: past, present and future. *Computers & Industrial Engineering*, 43(1), 231-249.
- MITRE. (2012a). Acquisition Risk Management Probability Definitions. Retrieved 19 December, 2012, from <http://www.mitre.org/work/sepo/toolkits/risk/StandardProcess/definitions/occurence.html>
- MITRE. (2012c). Risk Management Toolkit. Retrieved 20 December, 2012, from <http://www.mitre.org/work/sepo/toolkits/risk/>
- Moon, I.-C. (2008). *Destabilization of Adversarial Organizations With Strategic Interventions*. Carnegie Mellon University, Pittsburgh.
- Morgan, G. P., & Lanham, M. J. (2012). [personal office interaction and whiteboard brainstorming].
- Musich, P. (2001). Navy-EDS Deal Hits Troubled Waters. *eWeek*. Retrieved from eWeek - Enterprise IT Technology News, Opinion and Reviews website: <http://www.eweek.com/print/c/a/IT-Management/NavyEDS-Deal-Hits-Troubled-Waters/>
- Musman, S., Temin, A., Tanner, M., Fox, D., & Pridemore, B. (2010). Evaluating the Impact of Cyber Attacks on Missions. McLean, VA 22102: MITRE.
- National White Collar Crime Center (NW3C). (2011). 2011 Internet Crime Report. Washington, D.C.: Internet Crime Complaint Center.
- Navarro, P., & Spencer, A. (2001). Assessing the Costs of Terrorism. *Milken Institute Review*, 17-31.
- NCA. (2013). *National Command Authority*. Fort Leavenworth, KS: Retrieved from <http://webcache.googleusercontent.com/search?q=cache:VgF63jnDTKoJ:usacac.army.mil/cac2/call/thesaurus/toc.asp%3Fid%3D21281+&cd=3&hl=en&ct=clnk&gl=us>.
- Niccolai, J. (2008). Cable Repairs Set Back by Second Undersea Break. *PCWorld*.
- NIST. (2012). Risk Management Framework (RMF) -- Frequently Asked Questions (FAQs), Roles and Responsibilities & quick Start Guides (QSGs). Retrieved 3 December, 2012, from <http://csrc.nist.gov/groups/SMA/fisma/Risk-Management-Framework/index.html>
- Norris, F. H., Stevens, S. P., Pfefferbaum, B., Wyche, K. F., & Pfefferbaum, R. L. (2008). Community resilience as a metaphor, theory, set of capacities, and strategy for disaster readiness. *American journal of community psychology*, 41(1-2), 127-150.

- North, M. J. (2000). An agent-based tool for infrastructure interdependency policy analysis (pp. 1-9): Argonne National Lab., IL (US).
- ns-2. The Network Simulator. Retrieved 29 January, 2013, from <http://www.isi.edu/nsnam/ns/>
- Nykodym, N., Taylor, R., & Vilela, J. (2005). Criminal profiling and insider cyber crime. *Digital Investigation*, 2(4), 261-267.
- Office of the Chief of Staff of the U.S. Air Force. (2012). United States Air Force Posture Statement. Retrieved 14 December 2012, 2013, from <http://www.posturestatement.af.mil/>
- Office of the Chief of Staff, U. S. A., Congressional Activities Division (DACs-CAD). (2012). The Army Posture Statement. Retrieved 14 December, 2012, from <http://www.army.mil/info/institution/posturestatement/>
- Office of the President of the United States. (2003). *Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection*. Washington, DC: Retrieved from <http://www.dhs.gov/homeland-security-presidential-directive-7>.
- OMNeT++ Community. (2012). OMNeT++ Network Simulation Framework. Retrieved 24 November, 2012, from <http://www.omnetpp.org/home/what-is-omnet>
- Orlikowski, W. J., & Gash, D. C. (1994). Technological frames: making sense of information technology in organizations. *ACM Transactions on Information Systems (TOIS)*, 12(2), 174-207. doi: 10.1145/196734.196745
- Padgett, J. F. (1980). Managing garbage can hierarchies. *Administrative Science Quarterly*, 25(4), 583-604.
- Pai, V. S., Aron, M., Banga, G., Svendsen, M., Druschel, P., Zwaenepoel, W., & Nahum, E. (1998). *Locality-aware request distribution in cluster-based network servers*. Paper presented at the ACM Sigplan Notices.
- Panzarasa, P., Carley, K. M., & Krackhardt, D. (2001). *Modeling Structure and Cognition in Organizations: A Meta-Network Computational Approach*. Paper presented at the CASOS Conference 2001, Pittsburgh, PA.
- Parker, T., Sachs, M., Shaw, E., & Stroz, E. (2004). *Cyber adversary characterization: Auditing the hacker mind*: Syngress Media Incorporated.
- Peerenboom, J., P., & Fisher, R. E. (2007, Jan. 2007). *Analyzing Cross-Sector Interdependencies*. Paper presented at the Hawaii International Conference on System Sciences (HICSS), Hawaii.
- Pereira, J. V. (2009). The new supply chain's frontier: Information management. *International Journal of Information Management*, 29(5), 372-379.
- Perlroth, N. (2012, 2 October). Google Warns of New State-Sponsored Cyberattack Targets. *New York Times*. Retrieved from <http://bits.blogs.nytimes.com/2012/10/02/google-warns-new-state-sponsored-cyberattack-targets/?pagewanted=print>
- Perrings, C. (1998). Resilience in the Dynamics of Economy-Environment Systems. *Environmental and Resource Economics*, 11(3), 503-520. doi: 10.1023/A:1008255614276
- Pflanz, M. A. (2012). *On the Resilience of Command and Control Architectures*. (Systems Engineering and Operations Research PhD), George Mason University, Fairfax, VA. Retrieved from <http://hdl.handle.net/1920/7490>
- Pflanz, M. A., & Levis, A. (2012). An Approach to Evaluating Resilience in Command and Control Architectures. *Procedia Computer Science*, 8, 141-146.

- Pfleeger, S. L., Predd, J. B., Hunker, J., & Bulford, C. (2010). Insiders Behaving Badly: Addressing Bad Actors and Their Actions. *IEEE Transactions on Information Forensics and Security*, 5(1), 169-179.
- Pimm, S. L. (1984). The complexity and stability of ecosystems. *Nature*, 307(5949), 321-326.
- Piper, P., & Ramos, M. (2006). A Failure to Communicate - Politics, Scams, and Information Flow During Hurricane Katrina. *Searcher*, 14(6). Retrieved from: http://www.infotoday.com/searcher/jun06/piper_ramos.shtml
- Pole, W. (2009). Web in trouble? The hidden cables under a Cornish beach feeding the world's internet. *Daily Mail Online*. Retrieved from: <http://www.dailymail.co.uk/home/moslive/article-1196775/Web-trouble-The-hidden-cables-Cornish-beach-feeding-worlds-internet.html>
- Quarantelli, E. L. (1988). Disaster crisis management: A summary of research findings. *Journal of Management Studies*, 25(4).
- Quinn, R. E., & Cameron, K. (1983). Organizational life cycles and shifting criteria of effectiveness: Some preliminary evidence. *Management Science*, 29(1), 33-51.
- Ralston, P. A. S., Graham, J. H., & Hieb, J. L. (2007). Cyber security risk assessment for SCADA and DCS networks. *ISA transactions*, 46(4), 583-594.
- REA Public Affairs. (2013). About resilience engineering. Retrieved 9 August 2013, 2013, from <http://www.resilience-engineering-association.org/>
- Reardon, M. (2009). Vandals blamed for phone and Internet outage. *cnet*. Retrieved from: http://news.cnet.com/8301-1035_3-10216151-94.html
- Reason, J. (1991). Disasters and human failure. In A. Taylor, Lane, D., & Muir, H. (Ed.), *Psychological Aspects of Disasters*: British Psychological Society.
- Reed, J. (2012). Did Chinese Espionage Lead to F-35 Delays? *DefenseTech*. Retrieved from DefenseTech website: <http://defensetech.org/2012/02/06/did-chinese-espionage-lead-to-f-35-delays/>
- Ren, Y., Carley, Kathleen M., & Argote, L. (2001). *Simulating the Role of Transactive Memory in Group Training and Performance*. Paper presented at the CASOS Conference 2001, Pittsburgh, PA.
- Reporter, W. (2012). Hurricane Sandy: Warren County cancellations, road closures and updates. *New Jersey News*. Retrieved from http://www.nj.com/warrenreporter/index.ssf/2012/11/hurricane_sandy_warren_county_3.html
- resilience. (Ed.) (2003) Collins English Dictionary - Complete and Unabridged. HarperCollins.
- resilience. (2012). Merriam-Webster. Retrieved 24 November, 2012, from <http://www.merriam-webster.com/dictionary/resilience>
- Ridgeway, C. L. (2006). Linking Social Structure and Interpersonal Behavior: A Theoretical Perspective on Cultural Schemas and Social Relations. *Social Psychology Quarterly*, 69(1), 5-16. doi: 10.1177/019027250606900102
- Rieger, C. G., Gertman, D. I., & McQueen, M. A. (2009, 21-23 May 2009). *Resilient control systems: Next generation design research*. Paper presented at the 2nd Conference on Human System Interactions (HSI), Catania, Italy.
- Rinaldi, S. M., Peerenboom, J. P., & Kelly, T. K. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems*, 21(6), 11-25. doi: 10.1109/37.969131

- Roberts, K. H. (1989). New challenges in organizational research: high reliability organizations. *Industrial Crisis Quarterly*, 3, 111-125. doi: 10.1177/108602668900300202
- Roberts, K. H. (1990). Some characteristics of high reliability organizations. *Organization Science*, 1(2), 17.
- Roberts, K. H., Rousseau, D. M., & La Porte, T. R. (1993). The culture of high reliability: Quantitative and qualitative assessment aboard nuclear powered aircraft carriers. *Journal of High Technology Management Research*.
- Romjue, J. L. (1984, May-June). The Evolution of the Airland Battle Concept. *Air University Review*, 12.
- Rotenburg, M., Schneier, B., McConnell, M., Zittrain, J., & Donovan, J. M. (2010). The cyber war threat has been grossly exaggerated [a panel debate]. Retrieved from: <http://intelligencesquaredus.org/debates/past-debates/item/576-the-cyber-war-threat-has-been-grossly-exaggerated>
- Roulo, C. (2012). Cybercom chief: U.S. unprepared for serious cyber attacks. *American Forces Press Service*. Retrieved from Air Force Print News Today website: http://www.af.mil/news/story_print.asp?id=123311659
- Rydenfält, C., Ek, Å., & Larsson, P. A. (2013). Safety checklist compliance and a false sense of safety: new directions for research. *BMJ Quality & Safety*. doi: 10.1136/bmjqs-2013-002168
- Saint-Charles, J., & Mongeau, P. (2009). Different relationships for coping with ambiguity and uncertainty in organizations. *Social Networks*.
- Saltysiak, T. I., & Levis, A. H. (2012). *Co-Design: Course of Action Integration Through Common Conceptual Model Building*. Paper presented at the 17th International Command and Control Research and Technology Symposium, Fairfax, VA. http://www.dodccrp.org/events/17th_iccrts_2012/post_conference/papers/065.pdf
- Schreiber, C., & Carley, K. M. (2005). Ineffective Organizational Practices at NASA: A Dynamic Network Analysis (I. o. S. R. I. School of Computer Science (SCS), Center for the Computational Analysis of Social and Organizational Systems (CASOS), Trans.). Pittsburgh, PA: Carnegie Mellon University, School of Computer Science, Institute for Software Research International.
- Schreiber, C., Singh, S., & Carley, K. M. (2004). *Construct - A Multi-agent Network Model for the Co-evolution of Agents and Socio-cultural Environments [Technical report] / Carnegie Mellon University School of Computer Science Institute for Software Research International CMU-ISRI-04-109* (pp. 31). Retrieved from http://www.casos.cs.cmu.edu/publications/papers/schreiber_2004_constructmultiagent.pdf
- Schwartz, M. (2012). Sewage Flows After Storm Expose Flaws in System. *New York Times*. Retrieved from http://www.nytimes.com/2012/11/30/nyregion/sewage-flows-after-hurricane-sandy-exposing-flaws-in-system.html?pagewanted=all&_r=0&pagewanted=print
- SEC. (2003). Written Statement of the U.S. Securities and Exchange Commission Concerning the Performance of the Securities Markets During the Northeast Power Outage and Hurricane Isabel (S. a. E. Commission, Trans.) (pp. 7). Washington, D.C.: Security and Exchange Commission (SEC).
- Sherry, S., Drew, C., & Drew, A. (1998). *Blind man's bluff: The untold story of American submarine espionage*: Perseus Books Group.

- Shin, T., & Garske, M. (2012). AT&T Cables Vandalized, \$250,000 Reward Offered for Information. 3. Retrieved from: <http://www.nbcsandiego.com/news/local/ATT-Cables-Cut-Vandalized-250000-Reward-Offered-159155295.html>
- Shrivastava, P. (1987). *Bhopal: Anatomy of a crisis*. New York: Ballinger.
- Siegel, C. A., Sagalow, T. R., & Serritella, P. (2002). Cyber-Risk Management: Technical and Insurance Controls for Enterprise-Level Security. *Information Systems Security*, 11(4), 33-49. doi: 10.1201/1086/43322.11.4.20020901/38843.5
- Skvoretz, J., & Fararo, T. J. (1995). The Evolution of Systems of Social Interaction. In B. Agger (Ed.), *Current Perspectives in Social Theory* (Vol. 15, pp. 275-299). Greenwich, CT: JAI Press.
- Smith, G. E., Watson, K. J., Baker, W. H., & Pokorski Ii, J. A. (2007). A critical balance: collaboration and security in the IT-enabled supply chain. *International Journal of Production Research*, 45(11), 2595-2613. doi: 10.1080/00207540601020544
- Smith, G. S. (2004). Recognizing and Preparing Loss Estimates from Cyber-Attacks. *Information Systems Security*, 12(6), 46-57. doi: 10.1201/1086/44022.12.6.20040101/79786.8
- Snediker, D. E., Murray, A. T., & Matisziw, T. C. (2008). Decision support for network disruption mitigation. *Decision Support Systems*, 44(4), 954-969. doi: dx.doi.org/10.1016/j.dss.2007.11.003
- Souza, P. (2011). President Obama Monitors the bin Laden Mission. Retrieved 3 December, 2012, from http://www.time.com/time/photogallery/0,29307,2069208_2271482,00.html
- Staff Writer. (2012a, 2012). Pearl Harbor - A Day of Infamy. Retrieved 20 December, 2012, from http://www.military.com/Resources/HistorySubmittedFileView?file=history_pearlharbor.htm
- Staff Writer. (2012c). Security experts admit China stole secret fighter jet plans. *The Australian*. Retrieved from The Australian - News website
- Stoneburner, G., Goguen, A., & Feringa, A. (Eds.). (2002). *NIST Special Publication 800-30: Risk management guide for information technology systems*. Washington, D.C.: National Institute of Standards and Technology.
- Swaminathan, J. M., Smith, S. F., & Sadeh, N. M. (1998). Modeling supply chain dynamics: A multiagent approach*. *Decision sciences*, 29(3), 607-632. doi: 10.1111/j.1540-5915.1998.tb01356.x
- Ter Wal, A. L. J., & Boschma, R. A. (2007). Co-evolution of firms, industries and networks in space. *Papers in Evolutionary Economic Geography*, Utrecht University.
- The Associated Press. (2005, 20 February). New Nuclear Sub Is Said to Have Special Eavesdropping Ability. *New York Times*. Retrieved from <http://www.nytimes.com/2005/02/20/politics/20submarine.html?pagewanted=print&position=>
- Thibodeau, P. (2010). Cyberattacks an 'existential threat' to U.S., FBI says
FBI official warns about increasing cyber-sophistication of rogue states, criminals. *Computerworld*. Retrieved from Computerworld website: http://www.computerworld.com/s/article/print/9173967/Cyberattacks_an_existential_threat_to_U.S._FBI_says?taxonomyName=Cybercrime+and+Hacking&taxonomyId=82
- Thornburgh, N. (2005, September 5, 2005). The Invasion of the Chinese Cyberspies (And the Man Who Tried to Stop Them). *Time*.

- Tierney, K., Bevc, C., & Kuligowski, E. (2006). Metaphors matter: Disaster myths, media frames, and their consequences in Hurricane Katrina. *The Annals of the American Academy of Political and Social Science*, 604(1), 57-81.
- Townsend, F. F. (2006). *The Federal Response to Hurricane Katrina Lessons Learned*. Washington, D.C.: Government Printing Office Retrieved from <http://library.stmarytx.edu/acadlib/edocs/katrinawh.pdf>.
- Tracey, J. B., & Tews, M. J. (2005). Construct validity of a general training climate scale. *Organizational Research Methods*, 8(4), 353-374. doi: 10.1177/1094428105280055
- Tushman, M. L., & Romanelli, E. (1985). Convergence and reorientation in organizational evolution. *Research in Organizational Behavior*, 7, 171-222.
- Tversky, A., & Kahneman, D. (1974). Judgment under uncertainty: heuristics and biases. *Science*, 185(4157), 1124-1131.
- U.S.-Canada Power System Outage Task Force. (2004). Final Report on the August 14th Blackout in the United States and Canada.
- U.S. Cyber Command Public Affairs. (2010). U.S. Cyber Command. Retrieved 2 May, 2011, from http://www.stratcom.mil/factsheets/Cyber_Command/
- US Department of Commerce. (2003). United States Frequency Allocations, The Radio Spectrum. In spectrum_wall_chart_aug2011.pdf (Ed.), (Vol. 5040 x 3225). Washington, DC: US Department of Commerce, National Telecommunications and Information Administration.
- USAF. (2005). *Air Force Instruction (AFI) 13-1AOC, Operational Procedures - Air and Space Operations Center (AOC)*. Langley AFB: HQ USAF/XOOY Retrieved from <http://www.af.mil/shared/media/epubs/AFI13-1AOCV3.pdf>.
- USAF. (2012). *Cyberspace Warfare Operations Capabilities (CWOC) - Technology Concept Demonstrations*. (BAA ESC 12-0011). Air Force Material Command, Electronic Systems Center Retrieved from <https://www.fbo.gov/utills/view?id=b01bc061e003530dbcad3be82a97bb77>.
- USHR. (2012). Federal Tort Claims Act. Retrieved 20 December, 2012, from <http://www.house.gov/content/vendors/leases/tort.php>
- van Heesch, D. (2014). Doxygen-Generate documentation from source code. Retrieved November, 2014, from <http://www.stack.nl/~dimitri/doxygen/>
- Wade, M., & Hulland, J. (2004). Review: The Resource-Based View and Information Systems Research: Review, Extension, and Suggestions for Future Research. *MIS Quarterly*, 28(1), 107-142. doi: 10.2307/25148626
- Wagenhals, L. W., & H., L. A. (2001). *Modeling Effects Based Operations in Support of War Games*. Paper presented at the 15th International Symposium on Aerospace/Defense Sensing, Internal Society for Optical Engineering, Proceeding of SPIE.
- Wagenhals, L. W., Levis, A. H., & McCrabb, M. B. (2003). *Effects Based Operations: a Historical Perspective for a Way Ahead*. Paper presented at the 8th Int'l Command and Control Research and Technology Symposium, Washington, DC.
- Wagenhals, L. W., & Wentz, L. K. (2003). *New Effects-Based Operations Models in War Games*. Alexandria, VA: George Mason University.
- Wallner, J. (2008). *Cyber Risk Management Encyclopedia of Quantitative Risk Analysis and Assessment*. John Wiley & Sons, Ltd.

- Wang, L., Pai, V. S., & Peterson, L. (2002). The effectiveness of request redirection on CDN robustness. *ACM SIGOPS Operating Systems Review*, 36(SI), 345-360. doi: 10.1145/844128.844160
- Wasserman, S., & Faust, K. (1994). Social Network Analysis. Retrieved from <http://www.google.com/search?client=safari&rls=en-us&q=Social+Network+Analysis&ie=UTF-8&oe=UTF-8>
- Wasserman, S., & Iacobucci, D. (1991). Statistical Modeling of One-Mode and Two-Mode Networks: Simultaneous Analysis of Graphs and Bipartite Graphs. *British Journal of Mathematical and Statistical Psychology*, 44(1), 13-43. doi: 10.1111/j.2044-8317.1991.tb00949.x
- Webber, R. E. (2010). *Mission Assurance, Changing the Mindset*. Paper presented at the Global Warfare Symposium, Beverly Hills, CA 90210. <http://www.afa.org/events/natlsymp/2010/scripts/101118-Webber.pdf>
- Wei, W., Pfeffer, J., Reminga, J., & Carley, K. M. (2011). Handling Weighted, Asymmetric, Self-Looped, and Disconnected Networks in ORA [Technical report] / Carnegie Mellon University School of Computer Science Institute for Software Research International CMU-ISR-11-113. Pittsburgh, PA: Carnegie Mellon University, School of Computer Science, Institute for Software Research International, Pittsburgh PA 15213.
- Weik, M. H. (1961). The ENIAC Story. *ORDNANCE, January-February*, 1.
- Westrum, R. (2006). A Typology of Resilience Situations. In E. Hollnagel, D. D. Woods, & N. Leveson (Eds.), *Resilience Engineering—Concepts and Precepts* (pp. 55-66). Burlington, VT: Ashgate Publishing Company.
- WFSB Staff. (2012). DPH announces boil water advisories for 82 water systems. Retrieved 19 December, 2012, from <http://www.wfsb.com/story/19974938/dph-announces-boil-water-advisories-for-82-water-systems>
- Wihl, L., Varshney, M., & Kong, J. (2010). *Introducing a Cyber Warfare Communications Effect Model to Synthetic Environments*. Paper presented at the The Interservice/Industry Training, Simulation & Education Conference (I/ITSEC).
- Williams, M. L., & Johnson, J. (1993). Social network structures: An ethnographic analysis of intravenous drug use in Houston, Texas. *Drugs & Society*, 7, 65-90.
- Woods, D. D., & Branlat, M. (2011). *How human adaptive systems balance fundamental trade-offs: Implications for polycentric governance architectures*. Paper presented at the Proceedings of the Fourth Resilience Engineering Symposium, Sophia Antipolis, France.
- Woods, W. (1975). What's in a link: Foundations for semantic networks. In D. B. a. A. Collins (Ed.), *Representation and Understanding: Studies in Cognitive Science* (pp. 35-82). New York, NY: Academic Press.
- Zeggelink, E. P. H., Stokman, F. N., & Van de Bunt, G. G. (1996). The Emergence of Groups in the Evolution of Friendship Networks. *Journal of Mathematical Sociology*, 21, 29-55.

Appendix 1 Definitions

Central Definitions

Below is a small collection of definitions essential to the dissertation. The next section is an alphabetical section that contains other definitions taken from various sources. When using sources, I choose to use, in order of precedence, National standards bodies' definitions (e.g., [CNSS](#)), Joint doctrine, Service Doctrine, and finally dictionary definitions.

Cyberspace

“A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. “(Joint Staff J7, 2010a)

There are a multitude of definitions of cyberspace, some of which go on to enumerate the types and quantities of people and organizations (e.g., owners, customers, criminals, script kiddies, organized crime syndicates, nation-states) as well as the various types and natures of equipment (e.g., telecommunications companies' ([TELCO](#)) routers, undersea fiber-optic cables, points of presence, sites' perimeter routers and firewalls, organizational terminals and other IT). Additionally, many computer and information security practitioners and researchers believe threat enumeration (e.g., hackers, espionage, military forces, and 'advanced persistent threats') is necessary; the nature of threat(s) are inputs into the decision process of resource allocation. Adhering to the base definition in established doctrine however retains a broader perspective on the problem than using additional descriptors.

This dissertation models various types of organizations that own, use, operate, maintain and defend internet-protocol (IP)-based communication networks as well as other forms of telecommunications IT to facilitate information exchange. It also uses stylized representations of computing systems (e.g., databases, servers, client terminals) without delving into the technical implementation of those systems, their protocols, or their inner-workings.

Contested Cyberspace

A human-built environment constantly, but irregularly, effected by people and natural processes that can, and do, negatively interfere with the designed and intended purpose of that environment.

Appendix 1 Definitions

Merriam-Webster defines ‘contested’ as the following:

to make the subject of dispute, contention, or litigation (contested, 2013).

As discussed earlier, this dissertation, as well as the generalized discussion of mission assurance and resilience, requires a slight broadening of the definition above. This change is necessary as natural causes can create the same effects of denial, degradation, and disruption on availability as human-driven disputation or contention—though I’ve not found a reasonable path that nature can use to inflect effects on integrity or confidentiality.

Mission Assurance

The plain English definition this dissertation will use is shown below:

Mission assurance means having a level of confidence in the resilience of an organization, its ability to recover from or adjust to cyber events, along one or more measurable dimensions.

The USAF developed a nondoctrinal definition of mission assurance that conveys its core intent that the USAF and its units can “fight through an attack” (Elder, 2008). Importantly, the decision makers that developed this approach were not information security (INFOSEC) or computer security (COMPUSEC) practitioners. These decision makers were operations generalists who, by long experience and exposure, have learned that the complex choreography of USAF’s many missions have a central core: successful execution of military operations. The situation is akin to the organizations (e.g., oil exploration) that have multiple subelements (e.g., HR, Finance, Logistics) that perform necessary, even critical functions, that are, fundamentally, not the primary *raison d’être* of the organization.

Within the USAF multi-dimensional approach, shown in [Figure 134](#), INFOSEC and COMPUSEC practitioners will note the overall effort subsumes traditional definitions of information assurance (IA) and computer network defense (CND).

[Figure 134](#) clearly links the technical components of cyber capabilities and infrastructures (lower left) with the traditional notions of physical security (lower right). It also links the systems (center orange triangle) with the people and organizations (upper right) that use those systems. This depiction helped USAF leadership accomplish two (2) simultaneous tasks. The first was to enlighten traditional leadership in multiple facets of mission assurance without overly technical vocabulary. The second, and as importantly, was to ensure traditional ‘cyber’

Appendix 1 Definitions

personnel remembered that cyber capabilities are a means to an end—that peoples’ and organizations’ missions must be resilient to contested cyber environments and leaders are assured of that resilience. This continued meaningful functioning in the face of adversity leads us to our next, related definition.

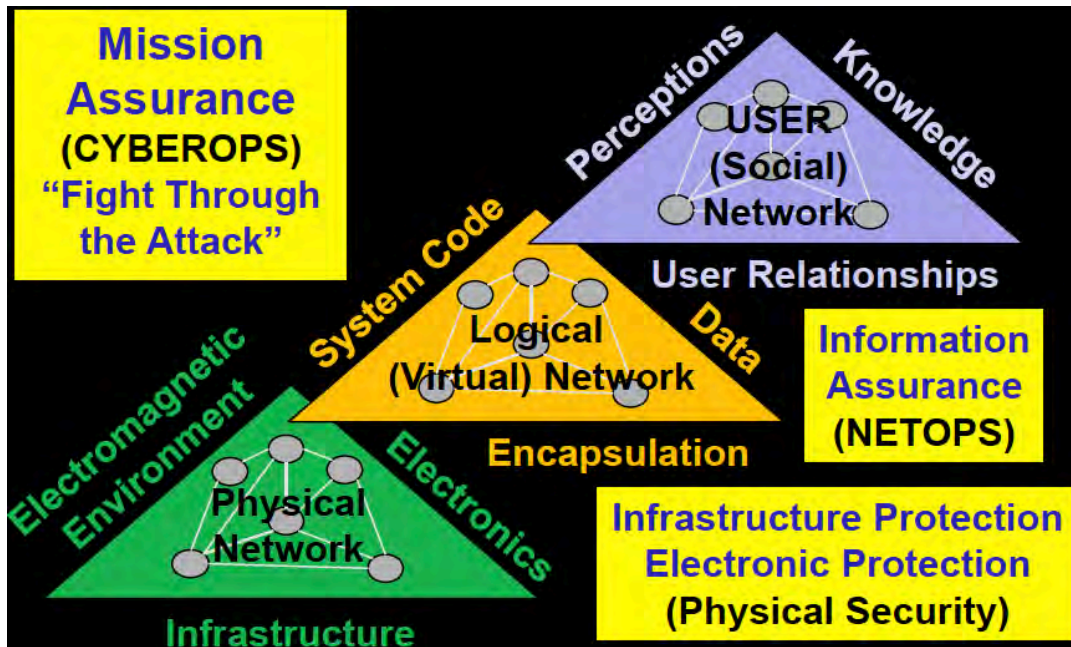


Figure 134: USAF Visual Depiction of Mission Assurance (Elder, 2008)

Resilience

Merriam-Webster defines ‘resilience’ as the following:

“an ability to recover from or adjust to misfortune or change” (resilience, 2012)

The nature of the misfortune or change is of course necessary to any discussion of resilience. The nature of who or what is being resilient, to what degree they are resilient to the misfortune, and how long they can demonstrate resilience are also essential to any analysis, assessment, and discussion of resilience. This dissertation contains both static structural assessments of resilience as well as dynamic assessments of resilience as a function of other measures.

“Contested cyber environments” helps scope the discussion to the type of misfortune or change, as does focusing solely on organizational resilience. A first impulse for many organizations concerning themselves with a ‘contested cyber environment’ is to leap to discussions of ‘bad people’ doing ‘bad things’ to the organizations’ computers and other IT resources. This initial impulse can also lead to follow-on questions, such as:

Appendix 1 Definitions

- To what degree do organizational subelements depend on their computers for their local needs? To what degree do local needs affect the organization-wide needs?
- Are the ‘bad people’ insiders to the organizations or outsiders?
- Are the ‘bad things’ malicious acts? Obviously nonmalicious acts? Somewhere in between? ‘Back-hoe’ attacks by road repair crews are generally not malicious while purposeful hacking generally is malicious. Self-infection with malware is generally insider carelessness leading to external exploitation, can be malicious, but intent is hard to trace or otherwise prove.
- Are off-site ‘bad things’ (e.g., power outages, telecommunications outages, solar-storms) considered part of a contested cyber environment? Are they considered at all when developing mission assurance plans and assessments for resilience to contested cyber environments?

From these examples, it’s possible to get a sense of a broad spectrum of events that can comprise a contested cyber environment. Indeed the spectrum of mechanisms of affect are so broad, it’s unlikely that any single model or simulation capability could adequately represent them. There is clearly value in exploring, via technically oriented modeling and simulation (M&S), specific effects by specific mechanisms in both general and specific situations. But exploring a broad spectrum of mechanisms and effects via such sampling is not the only method for researchers and organizational planners. Indeed, this dissertation has one goal of allowing such broad exploration without the per-attack mechanism details being present in the model—supporting generalization of impact assessments!

Since the dissertation is not exploring per-attack buffer overflows, cryptographic attacks, denial of service (DoS) or distributed DoS (DDoS) mechanisms, the reader is probably interested in knowing what the dissertation will explore. The briefest answer is that the dissertation explores the effects of these various mechanisms, without the mechanisms themselves having explicit representation. Using the CNSS’ now common acronym of confidentiality, integrity, and availability (CIA) (2010), it is feasible to consider the effects of nearly every form of computer network attack (CNA) disruption, degradation, denial, destruction (Joint Staff J7, 2010a) or deception (USAF, 2012)) within a contested cyber environment. A mechanism may create effects in one or more of these ontological categories, relieving the modeler and simulationist from the need to simulation specific technical mechanisms and specific technical effects, and instead recreate these primary effects within the IA ontology of confidentiality, integrity, and availability.

Appendix 1 Definitions

Like (Pflanz, 2012; Pflanz & Levis, 2012) a visual chart depicting the dynamic nature of resilience is useful to convey a more complete understanding.

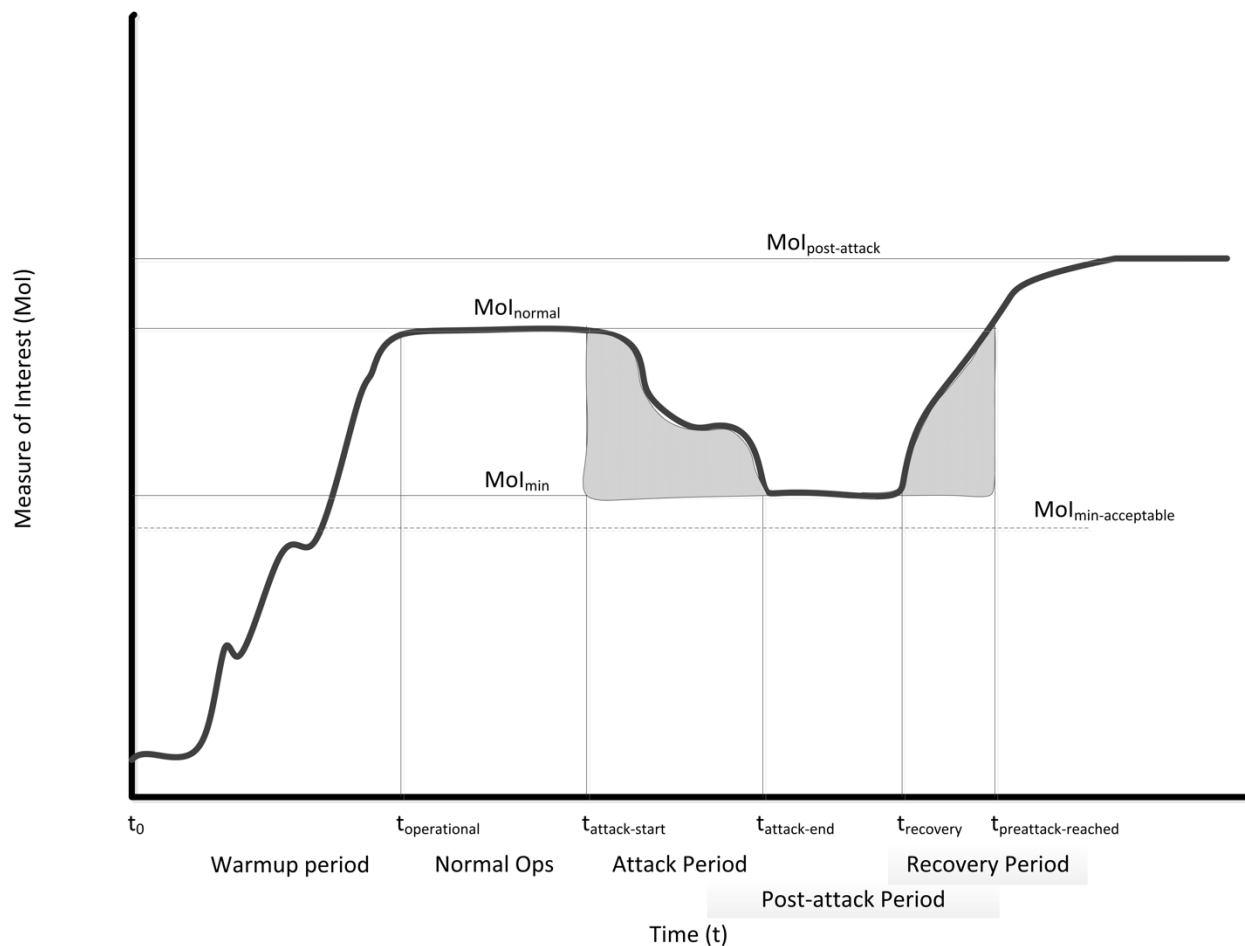


Figure 135: Dynamic visualization of resilience for an arbitrary measure of interest (MoI)(Morgan & Lanham, 2012)

In this picture, there is the span of time from t_0 to t_{warmup} that reflects the possible values of an MoI prior to reaching a pre-contested-environment equilibrium. As noted by Pimm (1984), without equilibrium, resilience is indefinable. During the time of normal operations ($\text{MoI}_{\text{normal}}$), there could be variance from the normal, though such variance over time would still need to establish equilibrium within some tolerances. The figure also depicts the beginning of an attack ($t_{\text{attack-start}}$), or some other form of cause for one of the CIA effects. While the attack is on going, the attack should be having some effect on the MoI, though it may not be consistent, statistically or operationally significant. As shown, there is an approximate stair step halfway through the attack...as just one of an infinite variety of possible impacts on the MoI (e.g. instantaneous drop, linear drop, logarithmic drop, quadratic drop). At some point-in-time, the attack ends ($t_{\text{attack-end}}$), though there is no guarantee that the organization or its agents are aware of the specific end

Appendix 1 Definitions

time—nor for that matter are they assured of being aware of a specific start time($t_{\text{attack-start}}$). The chart above depicts a quiescent period after the attack and before ‘recovery’ begins (t_{recovery}), or before the MoI rises above the minimum performance reached as a consequence of the attack. There is no requirement for recovery to start immediately, as the attack may have effects on the MoI that outlast the attack itself. It’s also important to note that there is a space between the minimum performance ($\text{MoI}_{\text{min-acceptable}}$) for this MoI and a minimally acceptable threshold set, *a priori*, by one or more leaders of organizations. This threshold may have been set, or may simply be a generalized statement by leadership akin to ‘no performance drop is acceptable!’ This picture does not depict a return to pre-attack levels for this MoI (at $t_{\text{pre-attack reached}}$), indeed there is no universal requirement in all definitions of resilience that this be so, notwithstanding Bishop (2011). Indeed, in the happy situation shown above, the forecast is that through adaptation, the attack/attacker makes the organization better in this MoI than they might otherwise have become.

In an attack, however, where the MoI_{min} drops below $\text{MoI}_{\text{min-acceptable}}$, the MoI for the modeled organization would have low resilience, and potentially low-survivability. Such a situation would make recovery all the more daunting as first recovery efforts would be geared to re-gaining the $\text{MoI}_{\text{min-acceptable}}$ level of performance.

It’s also feasible that there are indirect measures of resilience for the organization. An example of such could be the cognitive load turbulence due to a contested-cyber environment. During a contested cyber environment, facing degradation, destruction, denial, or disruption of a cyber resource, people will attempt to adapt. Part of their adaptation can be changes to their normal patterns of interaction with other systems and other agents. This change in interaction is an indirect measure of resilience—with very few changes, the effects of the contested cyber environment may be mitigated by the agents. Or the attack could provoke very large changes in interaction patterns. Once the attack has passed, it is unlikely that new interaction patterns recently experienced will *en masse* return to their pre-attack patterns. In this case, we would expect resilience to appear something like the figure below.

The measure of organization (MoO) shown on the vertical axis could, as discussed, be the stability of the cognitive core of activated alters for the decision makers (e.g., the members of the C-Suite). During the attack there is a decrease in stability of those activated cores, and importantly, even after the attack the stability continues to drop. However, after MoO_{min} is

Appendix 1 Definitions

reached, recovery commences and begins an upward trending but periodic improvement. In the case depicted, the new equilibrium is below the original equilibrium, indicating a permanent effect ($\text{MoO}_{\text{perm neg effect}}$) for this attack. If this effect is forecast to be large, a decision maker could use the forecast to potentially make changes in their continuity of operations planning, their rehearsals, or other ways to improve their ability to return to normal operations ($\text{MoO}_{\text{normal}}$). We expect to see the periodic nature of improvement prior to equilibrium as a reflection of the echoes of the original change—much as sound waves do not instantly dissipated, the perturbations of organizational adaptation will also not instantly remove themselves from the organization.

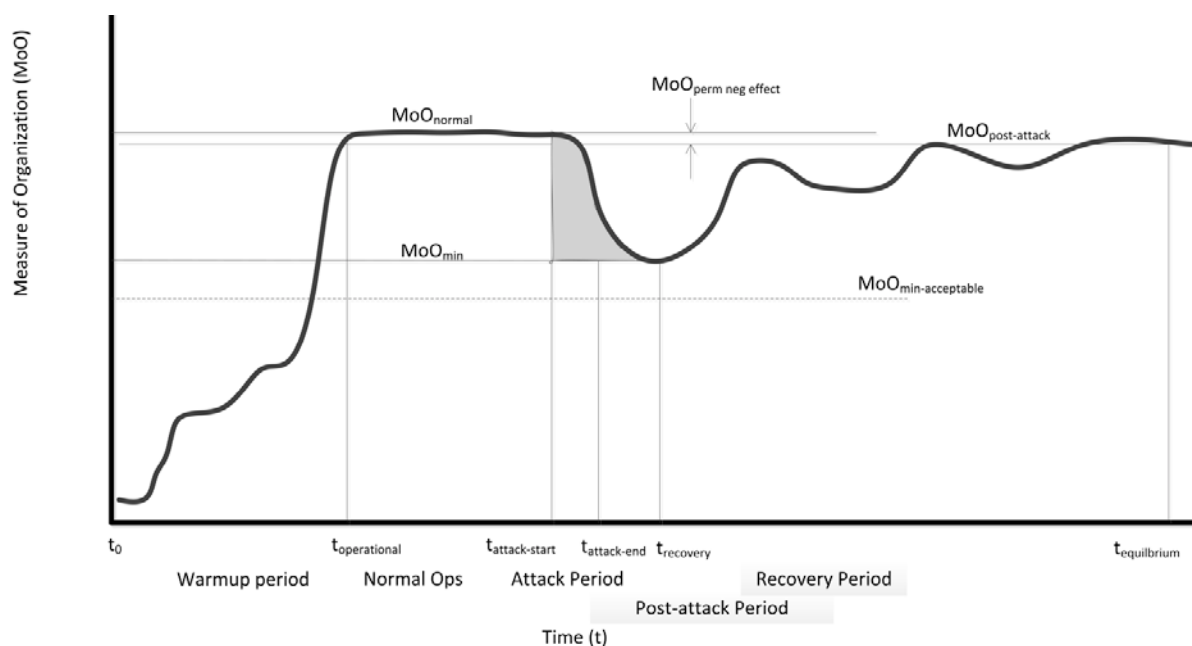


Figure 136: Dynamic visualization of resilience for an arbitrary measure of organization (MoO)(Morgan & Lanham, 2012)

Alphabetical Definitions

Computer Network Attack (CNA)

“Actions taken through the use of computer networks to disrupt, deny, degrade, or destroy [emphasis added] information resident in computers and computer networks, or the computers and networks themselves.” (Joint Staff J7, 2010a)

Computer Network Defense (CND)

“Actions taken to defend against unauthorized activity within computer networks. CND includes monitoring, detection, analysis (such as trend and pattern analysis), and response and restoration activities” (CNSS, 2010)

Appendix 1 Definitions

Computer Security (COMPUSEC)

“The protection resulting from all measures to deny unauthorized access and exploitation of friendly computer systems.” (Joint Staff J7, 2010a)

Information Security (INFOSEC)

“The protection of information and information systems against unauthorized access or modification of information, whether in storage, processing, or transit, and against denial of service to authorized users.” (Joint Staff J7, 2010a)

Information Assurance (IA)

“Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. These measures include providing for restoration of information systems by Incorporating protection, detection, and reaction capabilities.” (CNSS, 2010; Joint Staff J7, 2010a)

From an operations generalist perspective, IA is a repeatable set of processes that enable informed risk management in the face of uncertainty and competing demands on limited resources.

Tactical level of warfare

“The level of war at which battles and engagements are planned and executed to achieve military objectives assigned to tactical units or task forces.” (CNSS, 2010; Joint Staff J7, 2010a)

Appendix 2 Literature Review Bibliometrics

Introduction

This appendix is to document the steps and methodology I used to collect information in support of the [Literature Review](#) portion of the dissertation that started on page 11. It is my intention to provide sufficient information and specificity that the reader may duplicate the process I used, and ideally arrive at similar if not identical results. I have made the outputs of the searches into data files and made them available on my personal web page at the following URL: <http://www.andrew.cmu.edu/user/mlanham/relatedLit>:

Process

The following is a high-level summary of the steps I used to gather and analyze the bibliometric data included earlier in the dissertation.

1. Use Google Scholar to conduct key word, key phrase, collocation, and Boolean-based searches.
2. Use a custom ECMA/JavaScript I wrote, [Google Scholar Citation Exporter](#)¹⁶, to mark citations as related to the dissertation. This was a subjective decision based on a number of factors. Those factors included: citation count, title concepts, summary concepts, author(s), and publication.
3. Iterate steps 1 and 2 across each of the query sets I developed.
4. Pre-process collected citations and citation links to reduce duplicates and ensure well formed columns of data. Copy citations' identifiers and citations' titles to a separate file for text-based analysis (i.e., Latent Dirichlet Analysis and Latent Semantic Analysis).
5. Import collected citations as Nodes into ORATM
6. Import collected citation links as Node links into ORATM
7. Conduct ORATM-based Analysis

Searches and Search Results

Each of the searches fell into a mental category based on my personal intuition as well as suggestions from fellow students and CASOS faculty. The categories are shown below, with the search strings for each category depicted for future replication. The hyperlinks to the results

¹⁶ This script is an extension, by permission, of [Mayank Lahiri](#)'s "Google ScholarTM Citation Exporter." In brief, the original script allows a user to select multiple Google ScholarTM returns and then display the co-citations of those selected results in a new window. The extension resolved fatal errors that accumulated over time as a result of Google changing the HTML used to render the results. The extension then gives the user the option of displaying the results in a comma-limited window with citations at the top, and citation links at the bottom. A user may then cut and paste this displayed information into other files for follow-on processing and analysis.

point to my [personal web page](#) on Carnegie Mellon Web Servers. Should, at some future point, CMU remove my personal web page from their servers, I will have moved a copy of that web site to a new locale—Google™ or other search engines should be able to find the site with little difficulty.

Organizational Resilience

1. organizational resilience -child –ecology Output: [pdf](#)
2. (measure OR assess) AND (organization OR organizational) AROUND(10) resilience - "occupational stress" –seismic –children –youth Output: [pdf](#)
3. organizational adaptation to (crisis OR attack OR degraded) –animal Output: [pdf](#)

Cyber Command and Control

4. (resilient OR adaptive) (centralized OR decentralized) command and control cyber environments -"natural resource" Output: [pdf](#)
5. military cyber ("command AND control" OR C2) degraded AROUND(3) environments Output: [pdf](#)

Cyber Security

6. cyber vulnerability military ("command AND control" OR C2) (measure OR assess) Output: [pdf](#)
7. cyber sociotechnical organization vulnerability -scada –power Output: [pdf](#)
8. military effects of cyber attacks US OR Korea OR Estonia OR Georgia OR Lithuania Output: [pdf](#)
9. cyber military "mission assurance" Output: [pdf](#)
10. (perceived OR perception) and (reliance OR reliant) and ("information technology" OR cyber) –teaching –patient –medicine –entertainment Output: [pdf](#)

Modeling and Simulation

11. agent based modeling simulation organizational resilience "information technology" -water –agriculture –genetic Output: [pdf](#)
12. "discrete event" (modeling OR simulation) organizational resilience "information technology" -water –agriculture –genetic Output: [pdf](#)
13. "system dynamics" (modeling or simulation) organizational resilience "information technology" -water –agriculture Output: [pdf](#)
14. "business process" (modeling or simulation) organizational resilience "information technology" -water –agriculture Output: [pdf](#)
15. model organization reaction to loss of IT Output: [pdf](#)

SNA and Resilience to Cyber Vulnerability

16. organization AROUND(5) modeling and simulation "text mining" topic –gene Output: [pdf](#)
17. sociotechnical system vulnerability modeling (cyber or "information technology") Output: [pdf](#)

Appendix 2 Literature Review Bibliometrics

18. sociotechnical AROUND(5) (modeling OR model) AROUND(15) simulation (cyber OR "information technology" Output: [pdf](#)
19. sociotechnical disaster model "information technology" preparedness Output: [pdf](#)
20. metanetwork organizational model "information technology" Output: [pdf](#)
21. author:elder cyber Output: [pdf](#) and [pdf](#)

HRO and Resilience to Cyber Vulnerability

22. ("High Reliability Organization" OR HRO) resilience Output: [pdf](#)
23. "Resilience Engineering"

Pre-processing Collected Data

This step principally involved the merging of the multiple takes from the queries depicted in the [Searches and Search Results](#) section, removing duplicates, and ensuring well-formed data in each column of the merged data files. For cells with entries clearly placed one or two cells left or right of where they should be, I simply moved them to their correct position. For cells with no data, or partial data, I left them as was and conducted additional merging and cleaning within ORA™.

The data files end up in two (2) distinct comma separated variable (CSV) files: one with the citations' information ([relatedLit Citations.csv](#), URL: http://www.andrew.cmu.edu/user/mlanham/relatedLit/relatedLit_Citations.csv) and one with the links between citations ([relatedLit Links.csv](#)), URL http://www.andrew.cmu.edu/user/mlanham/relatedLit/relatedLit_Links.csv.

Importing Collected Data into ORA™

Metanetwork Creation and Preparation

1. Created a new, empty, metanetwork, which I called Dissertation Related Literature

Created the following node sets, with 1 node per node set as a place holder

- 1.1. Author (as ORA™ type Agent)
- 1.2. Article (as ORA™ type Resource)
- 1.3. Journal (as ORA™ type Organization)
- 1.4. Publisher (as ORA™ type Organization)
- 1.5. Year (as ORA™ type Event)

Created the following networks to link the node sets, though they are all empty

- 1.6. Article x Article
- 1.7. Author x Article
- 1.8. Journal x Article

Appendix 2 Literature Review Bibliometrics

1.9. Publisher x Journal

1.10. Year x Article

Import Node Sets and Networks

Article Node Set (IDs only) and Article x Article Network

To import the citation node identifiers, as well as import the links between the identifiers, I imported the `relatedLit_Citations.csv` first and had ORA™ create nodes in the Article node set for each unique ID it processed.

1. Within ORA™, selected the Article x Article
2. Selected from the menu, File→Data Import Wizard...
 - 2.1. Selected the option labeled Import Excel or text delimited files
 - 2.2. Selected the option labeled Table of network links
 - 2.3. Selected the button labeled Next
 - 2.4. Selected the option labeled Add to the existing metanetwork: and ensured I selected Dissertation Related Literature
 - 2.5. Selected the button labeled Next
 - 2.6. To the right of the Step 1 dialog box, I selected Browse and navigated to where I had stored the `relatedLit_Links.csv` file
 - 2.7. In the Step 2 portion of the UI
 - 2.7.1. Selected CITEDBY and CITED
 - 2.7.2. Set the type in each column to Resource
 - 2.8. In the Step 3 portion of the UI
 - 2.8.1. Selected the button labeled New to define a new network of links
 - 2.8.2. Selected `citedBy` in the Source Node Name column
 - 2.8.3. Selected `cited` in the Target Node Name column
 - 2.8.4. Selected `link` in the Link Value column
 - 2.8.5. Typed Article x Article in the Network Name column
 - 2.8.6. Placed a check mark in the Create new nodes for unrecognized node names
 - 2.9. Selected the button labeled Finish
 - 2.10. Selected from the menu, File→Save

For readers interested in performing the steps from [2.6](#) to [2.8](#) using a saved configuration file, save the source code listed under the subheading [Article x Article](#) within the section entitled [Error! Reference source not found.](#) to an XML file. Select that file using the Load configuration file button to automatically perform (or repeatedly perform) steps from [2.6](#) to [2.8](#).

Article Nodes' Attributes

Next I finished the importation of all the citations' attributes and information stored in the `relatedLit_Citations.csv` file.

1. Selected the Article node set
3. Selected from the menu, File→Data Import Wizard...
 - 3.1. Selected the option labeled Import Excel or text delimited files
 - 3.2. Selected the option labeled Table of node attributes
 - 3.3. Selected the button labeled Next
 - 3.4. Selected the metanetwork to modify by placing a check mark in the box next to the Dissertation Related Literature metanetwork name.
 - 3.5. Selected Next
 - 3.6. To the right of the Step 1 dialog box, I selected Browse and navigated to where I had stored the `relatedLit_Citations.csv` file
 - 3.7. In the Step 2 portion of the UI, I Selected `citationId` in the drop down box for Use this column for node names
 - 3.8. In the Step 3 portion of the UI
 - 3.8.1. For the `citationUrl` column, changed the type to URI
 - 3.8.2. For the `citedByUrl` column, changed the type to URI
 - 3.8.3. For the `relatedArticlesUrl` column, changed the type to URI
 - 3.8.4. For the `clusteredArticles` column, changed the type to URI
 - 3.8.5. For the `clusteredArticles` column, changed the type to URI
 - 3.8.6. For the `title` column, changed the type text
 - 3.8.7. For the `citedByCount` column, changed the type Number
 - 3.8.8. De-selected `journal` column
 - 3.8.9. De-selected `publisher` column
 - 3.8.10. De-selected `year` column
 - 3.8.11. De-selected `author0` to `author5` columns
 - 3.8.12. De-selected `link` column
 - 3.8.13. Selected Create new nodes for unrecognized node names. This selection will support the creation of nodes that were not in the links file, that are otherwise isolates in the citation metanetwork.
 - 3.9. In the Step 4 portion of the UI
 - 3.9.1. Selected the button labeled Clear All
 - 3.9.2. Selected the Article nodeset
 - 3.10. Selected the button labeled Finish
 - 3.11. Selected the button labeled OK in the window that popped up reporting the import status.
 - 3.12. Selected from the menu, File→Save

There is no saved configuration file for this step like there was for importing a network.

Author x Article Network

4. Selected the Author x Article
5. Selected from the menu, File→Data Import Wizard...
 - 5.1. Selected the option labeled Import Excel or text delimited files
 - 5.2. Selected the option labeled Table of network links
 - 5.3. Selected the button labeled Next
 - 5.4. Selected the option labeled Add to the existing metanetwork: and ensured I selected Dissertation Related Literature
 - 5.5. Selected the button labeled Next
 - 5.6. To the right of the Step 1 dialog box, I selected Browse and navigated to where I had stored the relatedLit_Citations.csv file
 - 5.7. In the Step 2 portion of the UI
 - 5.7.1. Selected CITATIONID, set the Class to Resource, and the Name to Article
 - 5.7.2. For AUTHOR0 to AUTHOR4, select the column
 - 5.7.2.1. Set the Class to Agent
 - 5.7.2.2. Set Name to Author
 - 5.8. In the Step 3 portion of the UI
 - 5.8.1. Selected the button labeled New to define a new network of links
 - 5.8.2. Selected author0 in the Source Node Name column
 - 5.8.3. Selected citationID in the Target Node Name column
 - 5.8.4. Selected link in the Link Value column
 - 5.8.5. Typed Author x Article in the Network Name column
 - 5.8.6. Repeat steps [5.8.1](#) to [5.8.5](#) for Author1 to Author4
 - 5.8.7. Placed a check mark in the Create new nodes for unrecognized node names
 - 5.9. Selected the button labeled Finish
 - 5.10. Selected from the menu, File→Save

For readers interested in performing the steps from [2.6](#) to [2.8](#) using a saved configuration file, save the source code listed under the subheading [Author x Article](#) within the section entitled [Error! Reference source not found.](#) to an XML file. Select that file using the Load configuration file button to automatically perform (or repeatedly perform) steps from [2.6](#) to [2.8](#).

Journal x Article Network

6. Selected the Author x Article
7. Selected from the menu, File→Data Import Wizard...
 - 7.1. Selected the option labeled Import Excel or text delimited files

Appendix 2 Literature Review Bibliometrics

- 7.2. Selected the option labeled Table of network links
- 7.3. Selected the button labeled Next
- 7.4. Selected the option labeled Add to the existing metanetwork: and ensured I selected Dissertation Related Literature
- 7.5. Selected the button labeled Next
- 7.6. To the right of the Step 1 dialog box, I selected Browse and navigated to where I had stored the relatedLit_Citations.csv file
- 7.7. In the Step 2 portion of the UI
 - 7.7.1. Selected CITATIONID, set the Class to Resource, and the Name to Article
 - 7.7.2. Selected Journal, set the Class to Organization, and the Name to Journal
- 7.8. In the Step 3 portion of the UI
 - 7.8.1. Selected the button labeled New to define a new network of links
 - 7.8.2. Selected journal in the Source Node Name column
 - 7.8.3. Selected citationID in the Target Node Name column
 - 7.8.4. Selected link in the Link Value column
 - 7.8.5. Typed Journal x Article in the Network Name column
 - 7.8.6. Placed a check mark in the Create new nodes for unrecognized node names
- 7.9. Selected the button labeled Finish
- 7.10. Selected from the menu, File→Save

For readers interested in performing the steps from [2.6](#) to [2.8](#) using a saved configuration file, save the source code listed under the subheading [Journal x Article](#) within the section entitled [Error! Reference source not found.](#) to an XML file. Select that file using the Load configuration file button to automatically perform (or repeatedly perform) steps from [2.6](#) to [2.8](#).

Publisher x Journal Network

I repeated the steps used to create the Journal x Article network making the appropriate substitutions for network and file names.

Year x Article Network

I repeated the steps used to create the Journal x Article network making the appropriate substitutions for network and file names.

Concept Nodeset, Text Nodeset and Semantic Network

1. Copied the Citation's Node Name and Node Title columns to a tab-delimited text file. The Node Name column contains the Google Scholar™ identifier for the citation, and the Node Title column contains the citation's title text as presented by Google Scholar™.
2. Used a small Java application, [CitationSplitter.java](http://www.andrew.cmu.edu/user/mlanham/code/CitationSplitter.java), (URL: <http://www.andrew.cmu.edu/user/mlanham/code/CitationSplitter.java>) to convert this text file into a directory containing a file per row in the text file. Each file uses the Node Name

as the file name, with an underscore ('_') prepended to avoid troubles with ID's using characters unacceptable to operating systems as a filename (e.g., a minus sign ('-') as the starting character).

3. Used AutoMap's Data-To-Model (D2M) (Kathleen M. Carley, Bigrigg, et al., 2011; Lanham et al., 2014; Lanham, Morgan, Carley, et al., 2011) process to ingest this directory of citation titles to create a concept list. The D2M wizard user interface (UI) is shown in [Figure 137](#). The concept list is a list of distinct words in the corpus of citation titles.
 - 3.1. I used a standard thesaurus available to CASOS researchers as well as a thesaurus I personally constructed over the course of multiple iterations of data reduction and cleaning. The personal AutoMap thesaurus is available the following URL http://www.andrew.cmu.edu/user/mlanham/relatedLit/relatedLit_Thesaurus.csv. I have no objections to future readers Incorporating this thesaurus into their work so long as they cite this dissertation within the relevant work.

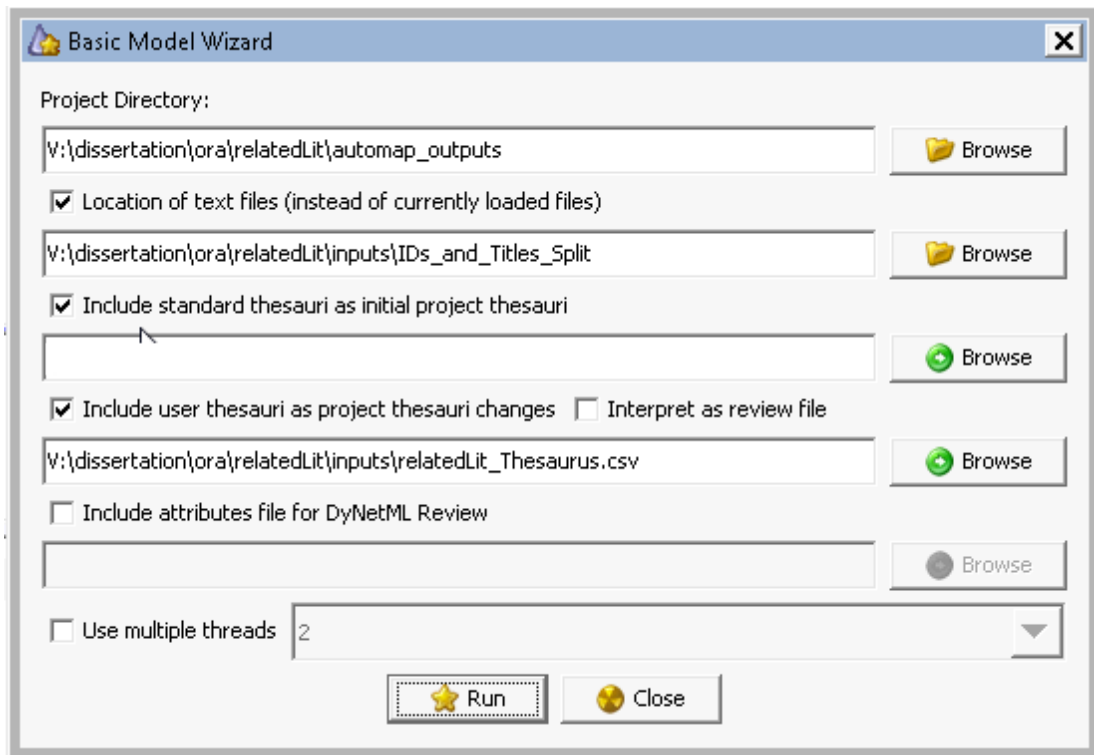


Figure 137: Data-to-Model (D2M) User Interface of AutoMap

After creation of the concept list, I 'cleaned' the concept list in support of creating semantic co-location networks of concepts in the corpus. The [D2M process](#), in addition to the concepts, provides the term-frequency inverse document frequency (TFIDF) as calculated using [Equation 49](#) through [Equation 51](#) (Kathleen M. Carley, Columbus, et al., 2011). The initial cleaning used the distribution of the TFIDF values depicted in [Figure 138](#) to establish a cut-off of 4.19×10^{-4} . This equates to including, in the first pass of cleaning, 90.442% of the concepts when sorted from largest to smallest TFIDF values, depicted in [Figure 139](#). The descriptive statistics for this pass are shown in [Table 60](#).

$$term_x \text{ frequency } (tf) = \frac{\text{Count of } term_x}{\text{Number of terms in } document_y} \quad (50)$$

Equation 49: Term Frequency for Concept x

$$\text{inverse document frequency (idf)} = \frac{\log(\text{number of documents in corpus})}{\text{number of documents with term}_x} \quad (51)$$

Equation 50: Inverse Document Frequency for Term x in Corpus

$$\text{TF-IDF} = \text{tf} \times \text{idf} \quad (52)$$

Equation 51: Term Frequency x Inverse Document Frequency (TFIDF)

Table 60: Descriptive statistics for D2M of Citation Titles

Description	Value	Description	Value
Number of Concepts, Pre-Cleaning	6,591	Number of Concepts, PostCleaning	4,276
TFIDF Mean	0.00088	TFIDF Standard Deviation	0.00187
TFIDF Median	0.00032	TFIDF Skew	6.59235
TFIDF Mode	0.00012	TFIDF Kertosis	63.0528
TFIDF Trend Equation ¹⁷	$y = 2.3563x^{-1.122}$	R2 for Trend Equation	0.9174
TFIDF Quartiles ¹⁸ (75%, 50%, 25%)	0.00617 0.00237 0.000849		

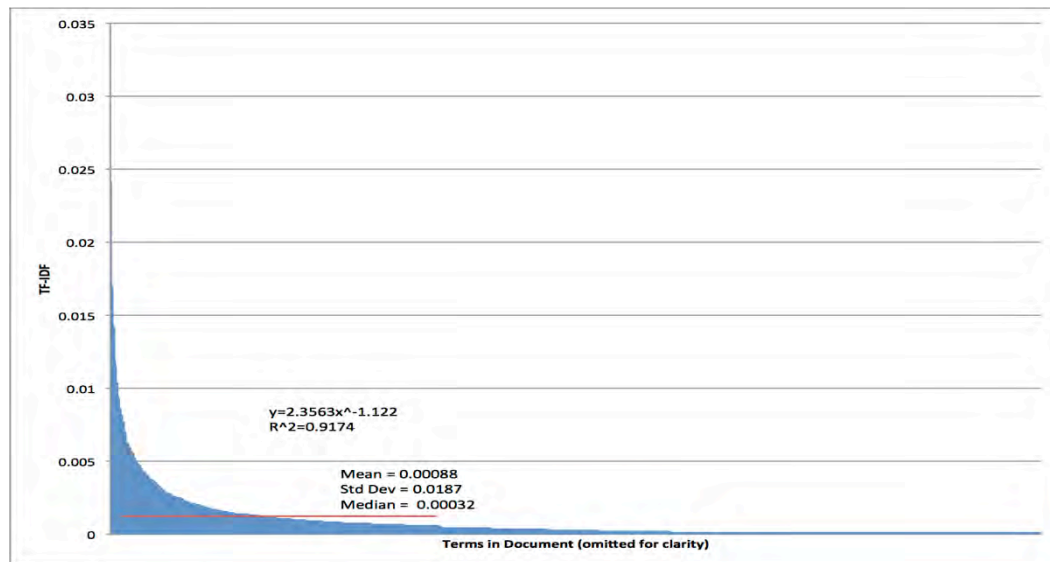


Figure 138: Concept¹⁹ x TFIDF²⁰

¹⁷ Using Excel for Mac 2010, 'Trend line' functionality built into Excel's Charting Functions

¹⁸ TFIDF values sorted in descending order, cumulatively summed until 25%, 50%, and 75% of the area under the curve is reached. 50th percent deviates from median as some TFIDF values repeat—many concepts have the same TFIDF values

¹⁹ Concepts not depicted in graph for visual clarity of the graph

²⁰ TFIDF values sorted in descending order

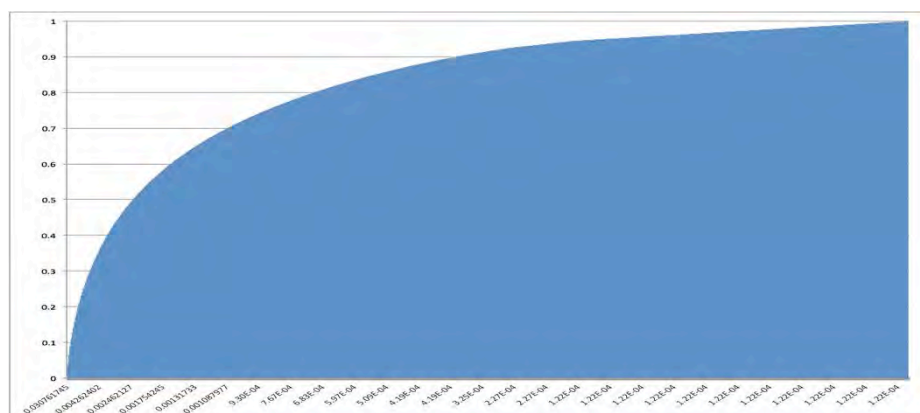


Figure 139: $TFIDF^{21} \times$ Cumulative Percentage of $\Sigma TFIDF$

- 3.2. The second pass of cleaning involved deleting concepts with a frequency of one (1) and then using ORA™ to remove isolates created from the previous steps.

Cleaned Article node set

1. Deleted articles with nonEnglish titles
2. Transformed networks to delete isolates based on entire metanetwork and saved as new file

Cleaned Author node set

1. Removed Asian script names
2. Used ORA™'s clean menu button to remove duplicates
3. Used ORA™'s Clean menu button to look for names 1 character edit-distance from others: An example would be M Lanham and MJ Lanham. Disambiguated with aid of scholar.google.com and google.com, ORA™ visualization, and ORA™ metrics. Merger if confident of names referring to the same individuals.
4. Used ORA™ Key Entity Report to look for any entries in top 50 that were visually similar. Used similarity to focus addition search for duplicates. Merged as necessary.
5. Transformed networks to delete isolates based on entire metanetwork and saved as new file

Cleaned Concept node set

1. Deleted concepts with UTF-8 symbols that were not rendered as meaningful text
2. Merged a number of nodes that were generalizations of each other
3. Ran Hot Topics Report on Semantic Network and had ORA™ depict the top 50 entries. The report depicted no entries that were generalizations of each other

Manipulate Networks

Co-Authors

1. Transposed Author \times Article
2. Multiplied Author \times Article with transpose to get co-authors

Articles per Year

1. Transposed Year \times Article

²¹ TFIDF values sorted in descending order

Appendix 2 Literature Review Bibliometrics

2. Multiplied Author x Article with transpose above to get articles per year

Move .edu organizations from Publisher to new nodeset School of type Organization

3. Selected *.edu and moved them to a new nodeset
4. Merged schools of same 2nd level domain unless I was aware of a 3rd level domain being a specific research lab/center

Move [BOOK] and [B] articles to new nodeset called Book of type Resource

5. Selected [BOOK|B] articles and moved them to a new nodeset

Move [C] articles to new nodeset called Citation of type Resource

6. Selected [C] articles and moved them to a new nodeset

Data-to-Model AutoMap ScriptRunner file

```
<?xml version="1.0" encoding="ISO-8859-1"?><Script>
<Utilities>
<Procedures>
  <DataToModel attributes="" numThreads="3"
projectDirectory="V:\dissertation\ora\relatedLit\automap_outputs"
standardThesaurus="**a unique to CASOS thesaurus**"
textDirectory="V:\dissertation\ora\relatedLit\inputs\IDs_and_Titles_Split"
userThesaurus="V:\dissertation\ora\relatedLit\inputs\relatedLit_Thesaurus.csv"/>
</Procedures>
<CEMap/>
<Extractors/>
<PreProcessing/>
<Generate/>
<PostProcessing/>
</Utilities>
<Settings>
<AutoMap deleteTemp="n" intermediate="y"
tempWorkspace="C:\temp\am3temp" textDirection="LT"
textDirectory="V:\dissertation\ora\relatedLit\inputs\IDs_and_Titles_Split" textEncoding="UTF-8"/>
</Settings>
</Script>
```

Article x Article

```
<?xml version="1.0" encoding="UTF-8"?>
<queryScript>
  <metaMatrix id="Meta Network">
    <create>
      <nodeset type="Resource" id="Article" />
      <nodeset type="Resource" id="Article" />
      <graph sourceNodesetId="Article" targetNodesetId="Article" id="Article x Article" />
    </create>
```

Appendix 2 Literature Review Bibliometrics

```
<query>
  <input> V:\dissertation \ora\relatedLit\relatedLit_Links.csv</input>
  <output>
    <graph id="Article x Article">
      <fromColumn index="0" makeUnique="false" />
      <toColumn index="1" makeUnique="false" />
      <weightColumn index="2" makeUnique="false" />
    </graph>
  </output>
</query>
</metaMatrix>
</queryScript>
```

Author x Article

```
<?xml version="1.0" encoding="UTF-8"?>
<queryScript>
  <metaMatrix id="Meta Network">
    <create>
      <nodeset type="Resource" id="Article" />
      <nodeset type="Agent" id="Author" />
      <nodeset type="Agent" id="Author" />
      <nodeset type="Agent" id="Author" />
      <nodeset type="Agent" id="Author" />
      <nodeset type="Agent" id="Author" />
      <graph sourceNodesetId="Author" targetNodesetId="Article" id="Author x
Article" />
      <graph sourceNodesetId="Author" targetNodesetId="Article" id="Author x
Article" />
      <graph sourceNodesetId="Author" targetNodesetId="Article" id="Author x
Article" />
      <graph sourceNodesetId="Author" targetNodesetId="Article" id="Author x
Article" />
      <graph sourceNodesetId="Author" targetNodesetId="Article" id="Author x
Article" />
    </create>
  <query>
    <input>V:\dissertation\ora\relatedLit\relatedLit_Citations.csv</input>
    <output>
      <graph id="Author x Article">
        <fromColumn index="10" makeUnique="false" />
        <toColumn index="0" makeUnique="false" />
        <weightColumn index="15" makeUnique="false" />
      </graph>
      <graph id="Author x Article">
        <fromColumn index="11" makeUnique="false" />
        <toColumn index="0" makeUnique="false" />
        <weightColumn index="15" makeUnique="false" />
      </graph>
      <graph id="Author x Article">
        <fromColumn index="12" makeUnique="false" />
        <toColumn index="0" makeUnique="false" />
        <weightColumn index="15" makeUnique="false" />
      </graph>
      <graph id="Author x Article">
        <fromColumn index="13" makeUnique="false" />
        <toColumn index="0" makeUnique="false" />
      </graph>
    </output>
  </query>
</queryScript>
```

Appendix 2 Literature Review Bibliometrics

```
<weightColumn index="15" makeUnique="false" />
</graph>
<graph id="Author x Article">
  <fromColumn index="14" makeUnique="false" />
  <toColumn index="0" makeUnique="false" />
  <weightColumn index="15" makeUnique="false" />
</graph>
</output>
</query>
</metaMatrix>
</queryScript>
```

Journal x Article

```
<?xml version="1.0" encoding="UTF-8"?>
<queryScript>
  <metaMatrix id="Meta Network">
    <create>
      <nodeset type="Resource" id="Article" />
      <nodeset type="Organization" id="Journal" />
      <graph sourceNodesetId="Journal" targetNodesetId="Article" id="Journal x
Article" />
    </create>
    <query>
      <input>V:\dissertation\ora\relatedLit\relatedLit_Citations.csv</input>
      <output>
        <graph id="Journal x Article">
          <fromColumn index="7" makeUnique="false" />
          <toColumn index="0" makeUnique="false" />
          <weightColumn index="15" makeUnique="false" />
        </graph>
      </output>
    </query>
  </metaMatrix>
</queryScript>
```

Publisher x Journal

```
<?xml version="1.0" encoding="UTF-8"?>
<queryScript>
  <metaMatrix id="Meta Network">
    <create>
      <nodeset type="Organization" id="Journal" />
      <nodeset type="Organization" id="Publisher" />
      <graph sourceNodesetId="Publisher" targetNodesetId="Journal" id="Publisher
x Journal" />
    </create>
    <query>
      <input>V:\dissertation\ora\relatedLit\relatedLit_Citations.csv</input>
      <output>
        <graph id="Publisher x Journal">
          <fromColumn index="8" makeUnique="false" />
          <toColumn index="7" makeUnique="false" />
          <weightColumn index="15" makeUnique="false" />
        </graph>
      </output>
    </query>
```

Appendix 2 Literature Review Bibliometrics

```
</metaMatrix>  
</queryScript>
```

Year x Article

```
<?xml version="1.0" encoding="UTF-8"?>  
<queryScript>  
  <metaMatrix id="Meta Network">  
    <create>  
      <nodeset type="Resource" id="Article" />  
      <nodeset type="Event" id="Year" />  
      <graph sourceNodesetId="Year" targetNodesetId="Article" id="Year x  
Article" />  
    </create>  
    <query>  
      <input>V:\dissertation\ora\relatedLit\relatedLit_Citations.csv</input>  
      <output>  
        <graph id="Year x Article">  
          <fromColumn index="9" makeUnique="false" />  
          <toColumn index="0" makeUnique="false" />  
          <weightColumn index="15" makeUnique="false" />  
        </graph>  
      </output>  
    </query>  
  </metaMatrix>  
</queryScript>
```

Appendix 3 Data to Model Implementation Details

Introduction

This appendix is to document the steps and methodology I used to collect and process information in support of rapidly developing the sociotechnical models of Strategic, Operational and Tactical set of US Department of Defense (DoD) commands. This material expands upon and extends the work briefly discussed in the [Data and Models](#) chapter of the dissertation that started on page 70. It is my intention to provide sufficient information and specificity that the reader may duplicate the process I used for each of the three (3) D2M generated models, and ideally arrive at similar if not identical results. I have made the Adobe Acrobat TM files (.pdf) available on my personal web pages at in three (3) zip files: [strategic.zip](#), [operational.zip](#), and [tactical.zip](#) at the following URL: <http://www.andrew.cmu.edu/user/mlanham/data2model>. I have also made the DoD-specific thesaurus, in what CASOS refers to as Master Thesaurus format, available as well as the model-specific thesauri. It is my intention that, for organizations who decide to use the [D2M process](#), these thesauri be available and useful. Additionally, as an employee of the USG, the work I have done while pursuing this research should be available to the public.

Retrieving input corpus

The bash shell script shown below retrieves the set of [PDF](#) documents for each model of interest in the dissertation. There were some documents that, though within the list of documents in later sections, I had to manually download as the organizations that host the documents have placed them behind authentication schemes that *wget* does not support.

Bash script for retrieval, text extraction, and text file splitting

The bash script is hosted on my personal web page at http://www.andrew.cmu.edu/user/mlanham/data2model/get_sets_as_text.sh and the algorithm for the script is below.

```
For each model in model list
  Create pdf directory, if needed
  Use wget to retrieve all entries in corpus_list.txt
  For each pdf file, use pdftotext to extract file_name.txt
  Create split_texts dir, if needed
  Move extracted text files to split_texts dir
```


Appendix 3 Data to Model Implementation Details

For each extracted text file, split it into 64KB chunks using split

List of documents for strategic level corpus and the URLs to retrieve them

1. http://www.dtic.mil/doctrine/doctrine/jwfc/esci_hbk.pdf
2. <http://www.dtic.mil/doctrine/doctrine/other/jopes.pdf>
3. <http://www.dtic.mil/doctrine/doctrine/other/nds2008.pdf>
4. http://www.dtic.mil/doctrine/doctrine/other/nms_2004.pdf
5. <http://www.dtic.mil/doctrine/doctrine/other/nss2010.pdf>
6. http://www.dtic.mil/doctrine/new_pubs/cjcsi5120_02b.pdf
7. http://www.dtic.mil/doctrine/new_pubs/jp1_0.pdf
8. http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf
9. http://www.dtic.mil/doctrine/new_pubs/jp1.pdf
10. http://www.dtic.mil/doctrine/new_pubs/jp2_0.pdf
11. http://www.dtic.mil/doctrine/new_pubs/jp2_01.pdf
12. http://www.dtic.mil/doctrine/new_pubs/jp2_03.pdf
13. http://www.dtic.mil/doctrine/new_pubs/jp3_0.pdf
14. http://www.dtic.mil/doctrine/new_pubs/jp3_01.pdf
15. http://www.dtic.mil/doctrine/new_pubs/jp3_05.pdf
16. http://www.dtic.mil/doctrine/new_pubs/jp3_06.pdf
17. http://www.dtic.mil/doctrine/new_pubs/jp3_07.pdf
18. http://www.dtic.mil/doctrine/new_pubs/jp3_08.pdf
19. http://www.dtic.mil/doctrine/new_pubs/jp3_09.pdf
20. http://www.dtic.mil/doctrine/new_pubs/jp3_10.pdf
21. http://www.dtic.mil/doctrine/new_pubs/jp3_11.pdf
22. http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf
23. http://www.dtic.mil/doctrine/new_pubs/jp3_14.pdf
24. http://www.dtic.mil/doctrine/new_pubs/jp3_16.pdf
25. http://www.dtic.mil/doctrine/new_pubs/jp3_17.pdf
26. http://www.dtic.mil/doctrine/new_pubs/jp3_24.pdf
27. http://www.dtic.mil/doctrine/new_pubs/jp3_27.pdf
28. http://www.dtic.mil/doctrine/new_pubs/jp3_29.pdf
29. http://www.dtic.mil/doctrine/new_pubs/jp3_30.pdf
30. http://www.dtic.mil/doctrine/new_pubs/jp3_31.pdf
31. http://www.dtic.mil/doctrine/new_pubs/jp3_32ch1.pdf
32. http://www.dtic.mil/doctrine/new_pubs/jp3_33.pdf
33. http://www.dtic.mil/doctrine/new_pubs/jp3_34.pdf
34. http://www.dtic.mil/doctrine/new_pubs/jp3_35.pdf
35. http://www.dtic.mil/doctrine/new_pubs/jp3_41.pdf
36. http://www.dtic.mil/doctrine/new_pubs/jp3_52.pdf
37. http://www.dtic.mil/doctrine/new_pubs/jp3_57.pdf
38. http://www.dtic.mil/doctrine/new_pubs/jp4_0.pdf
39. http://www.dtic.mil/doctrine/new_pubs/jp4_01.pdf
40. http://www.dtic.mil/doctrine/new_pubs/jp4_07.pdf
41. http://www.dtic.mil/doctrine/new_pubs/jp4_08.pdf
42. http://www.dtic.mil/doctrine/new_pubs/jp5_0.pdf
43. http://www.dtic.mil/doctrine/new_pubs/jp6_0.pdf

Appendix 3 Data to Model Implementation Details

44. http://www.dtic.mil/doctrine/training/cjcsn3500_01.pdf
45. http://www.dtic.mil/doctrine/training/cjcsn3500_01.pdf
46. http://www.dtic.mil/doctrine/training/joh_aug2010.pdf
47. http://www.dtic.mil/doctrine/training/ujtl_tasks.pdf
48. http://www.dtic.mil/futurejointwarfare/concepts/approved_ccjov3.pdf
49. https://jdeis.js.mil/jdeis/new_pubs/jp3_05_1.pdf
50. https://jdeis.js.mil/jdeis/new_pubs/jp3_09_3.pdf
51. https://jdeis.js.mil/jdeis/new_pubs/jp3_13_1.pdf
52. https://jdeis.js.mil/jdeis/new_pubs/jp3_13_3.pdf
53. https://jdeis.js.mil/jdeis/new_pubs/jp3_13_4.pdf
54. https://jdeis.js.mil/jdeis/new_pubs/jp3_15_1.pdf
55. https://jdeis.js.mil/jdeis/new_pubs/jp3_60.pdf
56. https://jdeis.js.mil/jdeis/new_pubs/jp4_012.pdf

List of documents for operational level corpus and the URLs to retrieve them

1. Air Force Instruction (AFI) 13-1AOCV3.pdf
2. Air Force Tactics Techniques and Procedures (AFTTP) 3-3.2 AOCNov07.pdf
3. http://static.e-publishing.af.mil/production/1/af_cv/publication/afdd1/afdd1.pdf
4. http://static.e-publishing.af.mil/production/1/af_cv/publication/afdd2-0/afdd2-0.pdf
5. http://static.e-publishing.af.mil/production/1/af_cv/publication/afdd3-0/afdd3-0.pdf
6. http://static.e-publishing.af.mil/production/1/af_cv/publication/afdd3-01/afdd3-01.pdf
7. http://static.e-publishing.af.mil/production/1/af_cv/publication/afdd3-04/afdd3-04.pdf
8. http://static.e-publishing.af.mil/production/1/af_cv/publication/afdd3-05/afdd3-05.pdf
9. http://static.e-publishing.af.mil/production/1/af_cv/publication/afdd3-10/afdd3-10.pdf
10. http://static.e-publishing.af.mil/production/1/af_cv/publication/afdd3-12/afdd3-12.pdf
11. http://static.e-publishing.af.mil/production/1/af_cv/publication/afdd3-13/afdd3-13.pdf
12. http://static.e-publishing.af.mil/production/1/af_cv/publication/afdd3-14/afdd3-14.pdf
13. http://static.e-publishing.af.mil/production/1/af_cv/publication/afdd3-17/afdd3-17.pdf
14. http://static.e-publishing.af.mil/production/1/af_cv/publication/afdd3-27/afdd3-27.pdf
15. http://static.e-publishing.af.mil/production/1/af_cv/publication/afdd3-40/afdd3-40.pdf
16. http://static.e-publishing.af.mil/production/1/af_cv/publication/afdd3-52/afdd3-52.pdf
17. http://static.e-publishing.af.mil/production/1/af_cv/publication/afdd3-60/afdd3-60.pdf
18. http://static.e-publishing.af.mil/production/1/af_cv/publication/afdd3-70/afdd3-70.pdf
19. http://static.e-publishing.af.mil/production/1/af_cv/publication/afdd6-0/afdd6-0.pdf
20. http://www.au.af.mil/au/awc/awcgate/jfcom/cc_handbook_sc_1sep2008.pdf
21. http://www.dtic.mil/doctrine/doctrine/jwfc/esci_hbk.pdf
22. <http://www.dtic.mil/doctrine/doctrine/other/jopes.pdf>
23. <http://www.dtic.mil/doctrine/doctrine/other/nds2008.pdf>
24. http://www.dtic.mil/doctrine/doctrine/other/nms_2004.pdf
25. <http://www.dtic.mil/doctrine/doctrine/other/nss2010.pdf>
26. http://www.dtic.mil/doctrine/new_pubs/cjcsi5120_02b.pdf
27. http://www.dtic.mil/doctrine/new_pubs/jp1_0.pdf
28. http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf
29. http://www.dtic.mil/doctrine/new_pubs/jp1.pdf
30. http://www.dtic.mil/doctrine/new_pubs/jp2_0.pdf
31. http://www.dtic.mil/doctrine/new_pubs/jp2_01.pdf
32. http://www.dtic.mil/doctrine/new_pubs/jp2_03.pdf

Appendix 3 Data to Model Implementation Details

33. http://www.dtic.mil/doctrine/new_pubs/jp3_0.pdf
34. http://www.dtic.mil/doctrine/new_pubs/jp3_01.pdf
35. http://www.dtic.mil/doctrine/new_pubs/jp3_05.pdf
36. http://www.dtic.mil/doctrine/new_pubs/jp3_06.pdf
37. http://www.dtic.mil/doctrine/new_pubs/jp3_07.pdf
38. http://www.dtic.mil/doctrine/new_pubs/jp3_08.pdf
39. http://www.dtic.mil/doctrine/new_pubs/jp3_09.pdf
40. http://www.dtic.mil/doctrine/new_pubs/jp3_10.pdf
41. http://www.dtic.mil/doctrine/new_pubs/jp3_11.pdf
42. http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf
43. http://www.dtic.mil/doctrine/new_pubs/jp3_14.pdf
44. http://www.dtic.mil/doctrine/new_pubs/jp3_16.pdf
45. http://www.dtic.mil/doctrine/new_pubs/jp3_17.pdf
46. http://www.dtic.mil/doctrine/new_pubs/jp3_24.pdf
47. http://www.dtic.mil/doctrine/new_pubs/jp3_27.pdf
48. http://www.dtic.mil/doctrine/new_pubs/jp3_29.pdf
49. http://www.dtic.mil/doctrine/new_pubs/jp3_30.pdf
50. http://www.dtic.mil/doctrine/new_pubs/jp3_31.pdf
51. http://www.dtic.mil/doctrine/new_pubs/jp3_32chl.pdf
52. http://www.dtic.mil/doctrine/new_pubs/jp3_33.pdf
53. http://www.dtic.mil/doctrine/new_pubs/jp3_34.pdf
54. http://www.dtic.mil/doctrine/new_pubs/jp3_35.pdf
55. http://www.dtic.mil/doctrine/new_pubs/jp3_41.pdf
56. http://www.dtic.mil/doctrine/new_pubs/jp3_52.pdf
57. http://www.dtic.mil/doctrine/new_pubs/jp3_57.pdf
58. http://www.dtic.mil/doctrine/new_pubs/jp4_0.pdf
59. http://www.dtic.mil/doctrine/new_pubs/jp4_01.pdf
60. http://www.dtic.mil/doctrine/new_pubs/jp4_07.pdf
61. http://www.dtic.mil/doctrine/new_pubs/jp4_08.pdf
62. http://www.dtic.mil/doctrine/new_pubs/jp5_0.pdf
63. http://www.dtic.mil/doctrine/new_pubs/jp6_0.pdf
64. http://www.dtic.mil/doctrine/training/cjcsn3500_01.pdf
65. http://www.dtic.mil/doctrine/training/cjcsn3500_01.pdf
66. http://www.dtic.mil/doctrine/training/joh_aug2010.pdf
67. http://www.dtic.mil/doctrine/training/ujtl_tasks.pdf
68. http://www.dtic.mil/futurejointwarfare/concepts/approved_ccjov3.pdf
69. <http://www.e-publishing.af.mil/shared/media/epubs/afdd3-03.pdf>
70. https://jdeis.js.mil/jdeis/new_pubs/jp3_05_1.pdf
71. https://jdeis.js.mil/jdeis/new_pubs/jp3_09_3.pdf
72. https://jdeis.js.mil/jdeis/new_pubs/jp3_13_1.pdf
73. https://jdeis.js.mil/jdeis/new_pubs/jp3_13_1.pdf
74. https://jdeis.js.mil/jdeis/new_pubs/jp3_13_3.pdf
75. https://jdeis.js.mil/jdeis/new_pubs/jp3_13_3.pdf
76. https://jdeis.js.mil/jdeis/new_pubs/jp3_13_4.pdf
77. https://jdeis.js.mil/jdeis/new_pubs/jp3_13_4.pdf
78. https://jdeis.js.mil/jdeis/new_pubs/jp3_15_1.pdf

79. https://jdeis.js.mil/jdeis/new_pubs/jp3_60.pdf

80. https://jdeis.js.mil/jdeis/new_pubs/jp4_012.pdf

Corpus augmentation

Augmenting corpus—figures to text

Figures within texts remain indecipherable to the *pdftotext* application as well as the AutoMap program. As such, the author and a collaborator, Jon Licht, translated select figures from AFTTP 13-3.2 to text for ingest by AutoMap and for use in previous work. Those figures were;

1.1	3.4	4.3	6.2
1.2	3.5	3.5	6.5
1.3	3.6	4.8	6.9
3.1	3.7	5.1	6.14
3.2	4.1	5.2	
3.3	4.2	5.5	

Though undoubtedly the generated models could benefit from translating other figures to text, there is at present insufficient evidence to assess the improvement. Many of the cross functional groups' relationships and membership depicted in AOC structural diagrams were not in the sets as text—thus substantiating the possible usefulness of figure-to-text translation. However, as discussed in the [Data and Models](#) chapter starting on page 70, it remains an open question if such effort will always work, will, with statistical significance, appropriately update models, or if, in the absence of statistical significance, provide qualitative improvements to the models.

Additionally, translating pictures into their respective “one thousand words” is a label intensive process that is clearly not aligned with the key word ‘Rapid’ in the title of the dissertation. Though figures and pictures remain relevant and useful to a large set of the human readers of doctrine, it is doubtful that they will provide meaningful assistance

Retrieving input corpus

Augmenting corpus—coercing links via AutoMap

ORA™ does not yet have the ability to capture a change list, a set of changes created by the user, for edges between nodes within the ORA™ UI. One way I captured additions of links between existing nodes was through the use of a manually created and updated *Isolate Correction* text file. This file, in pseudo-English, supports the automated creation of links between multiple node types using either the reduced form name of a node (e.g., i_t) or other forms that the thesaurus is ready to process correctly (e.g., information technology). Through the deliberate creation of sentences with words that should be linked to create an accurate model, AutoMap can be manipulated into creating links a researcher would otherwise have to create by hand. In this way, a modeler can reduce deficiencies in the model AutoMap generates from the corpus of text.

This technique, like the figures-to-text translation discussed above, has its drawbacks. It is easy, and sometimes entirely appropriate to hand-link dozens to hundreds of nodes to other nodes—even if not readily repeatable by other researchers attempting to replicate and extend work. It is also easy, sometimes appropriate to type the relationships in sentences knowing the names of the nodes and the word(s) that capture the relationship link between the nodes. This process has the advantage of being repeatable for future researchers, as well as slowly building up a repository of relationships explicitly drawn in figures, but frequently not addressed as text. The final draw back for this technique is the labor drain to author the links-as-sentences file. Such labor drain runs contrary to the rapid initial model creation implied in the dissertation model. It may however be suitable for model sustainment and refinement over time.

Pre-processing DoD corpus

Over the course of the dissertation, there were several opportunities to refine the process and reduce the amount of thesaurus refinement and ORA™-based model refinement. This section addresses each of those opportunities and the techniques I used to conduct pre-processing of the corpus before using AutoMap.

Regular expression deletion of noise patterns

Many of the documents in the corpus have headers or footers that contain verbiage that, if retained in the final models, would unduly weight the repeated concepts. There are also other word patterns that AutoMap, as of 2013, is incapable of removing or adequately addressing. To resolve this situation, I used bash shell code below to invoke perl and pre-process the corpus to replace the identified patterns with empty white space. Having a script available and functioning reduces the development time for future researchers and / or organizations desirous of using this dissertation's process. The overhead in terms of processing time was minimal, on the order of a few minutes per corpus.

```
#!/usr/bin/sh
#
#3rd pattern catches Doc Origination +
# number [.number[alpha][.][number]]
#4th pattern catches Title + number, USC, Section +
# Number Doc Original + number, doc-title
#5th pattern cleans up multiple underscores to
# single underscore
#6th pattern drops trailing underscores from words
#7th pattern drops leading underscores from words
#8th pattern drops patterns of junk chars created(?)
# during pdf-to-txt conversion
perl -0744pi -e \
's/Department of Defense Instruction \ (DODI\ ) /DODI/g;\
s/Joint Publication|Joint Publication\w*\JP\ ) /JP/g;\
s/(EO|HSPD|PDD|CJCSI|NSPD|DODD|DODI|JP|AR|AFDD|FM|TC|DIAM
|CJCSN|CJCSM|AFTTPI|DCID|AFDDs|j_p|DODDs|APP|STANAG|TM) [
-.]?([0-9]+) (?:[.-] ([0-9]*)) ? ([A-Z]*) (?:[.-] ([0-
9]+)) ? (?:[.-] ([A-
Z]+)) ? (, ([^\r\n.]* (\r[^\r\n,]*) {0,2}) [.,]) ?/lc($1)."_$2_
$3_$4_$5"/gie;\
s/(Title) ([0-9]+) (\, ? USC\, ? (?:Section ([0-
9]+)) ? [^\r\n.]* (\r[^\r\n,]*) ? \.) ?/lc($1)."_$2_$4"/gie;\
s/_+/_/g;\
s/_b_/g;\
s/_\b//g;\
s/^Table.*[0-9]+$/g;\
s/^Figure.*[0-9]+$/g;\
s/[ÔøÔΩ, Äç≈√ æ¬©\?]/ /g;' $1
```

Case sensitive application of DoD and model-specific thesaurus

Since the DoD makes extensive use of acronyms, I needed to have a case sensitive way of disambiguating all-capital-letter acronyms from words that might otherwise be in the thesaurus. To conduct the disambiguation, I applied the DoD thesaurus in a case sensitive manner, using a short Python script whose pseudo-code is below—the actual python script is on my personal web page at

<http://www.andrew.cmu.edu/user/mlanham/code/applyAcronymThesaurus.py>.

The Python script performs word-level, case sensitive, regular expression matching as well as attempting to match words surrounded by parenthesis. The DoD uses a writing style where authors spell out an acronym then specify the acronym in parenthesis (e.g., Listening Post (LP)). The script also performs a function that AutoMap developers have sense incorporated—turning hyphenated words into ngrams as a first-pass heuristic for ngram identification.

```
read thesaurus into Python key-value dictionary
for each text file
  for each line of text
    for each word in line
      if word in thesaurus
        if meta-ontology column == #delete
          delete word in line
        else replace word in line with
          thesaurus word
      else if word minus 1 char in thesaurus
        if meta-ontology column == #delete
          delete word in line
        else replace word in line with
          thesaurus word
      if word contains hyphen
        convert word to ngram
flush read/writer buffers periodically
```

Metanetwork encoding heuristics for thesaurus refinement

The thesaurus refinement process is rife with opportunities for inconsistencies. Though follow-on researchers may choose to disagree with the encoding choices I have made, the table below depicts the heuristics I used when assigning concepts of interest to one of the ontological categories in the metanetwork framework.

Appendix 3 Data to Model Implementation Details

Table 61: Metanetwork ontological labeling heuristics

Key word/words in original text segment	Metanetwork ontology category
Most words with –ly, -est suffixes	Attribute (based on generalization that the words with those endings are adverbs)
Most words with –ed suffix	Knowledge (based on generalization that the past-tense of a verb implies knowledge of the execution of that verb)
Ranks (SES, GS, E1-E9, O1-O10)	Attribute
Request, Responsibilities, Duties	Task
Chief, commander, director, system, processor, tool, database Specific named people relevant to project, Specific named position within orgs filled by exactly one person (e.g. Commander, Director, Secretary)	Agent
Authority (Ability to grant/deny permission)	Resource
Critical	Belief
Conference	Event
Agreement, architecture, consequence, contract, course, Estimate, guide, handbook, instruction*, law, memo*, message, mission, Module, *plan, policy, report, treaty, *authority	Knowledge Resource
Shared information, if when given to another, the originator still has the information (e.g., lists, opords, plans, oplans, procedures)	Knowledge
Area, Facility, installation, base, operations area, post, camp, station	Location
Program	Task (e.g. WMD Counter-proliferation), sometimes organization when I can tie the lone word into a N-Gram for disambiguation

Appendix 3 Data to Model Implementation Details

<p>Agency, branch, brigade, center, committee, company, council, detachment, division, fleet, MEU, MEB, Mission, office for *, office of *, organization, platoon, program office, *service*, named units/organization/ship, squadron, team, united, wing, ship(s), S1-S9, G1-G9, same for A/N/M/J-staff codes</p> <p>Specific/named (e.g. fighter wing, division, brigade, agency) collection of people or organizations (by composition or aggregation), * force(s), alliance</p>	<p>Organization (specific ships, when discussed as a resource [e.g. USS JFK was decommissioned/overhauled) get coded as “resource” instead of org)</p>
<p>Generic/unnamed (e.g. fighter wing, division, brigade, agency) collection of people or organizations (by composition or aggregation), * force(s), alliance</p>	<p>Resource</p>
<p>Causeway, equipment, radios, antenna, fuel, medal, missile, package, * Program (e.g. Contingency Program, DITSCAP, DIACAP), tanks, trucks, airplanes, programme</p> <p>An instance of a physical asset, if when given to another, the originator no longer has it AND the asset is not frequently synonymous with an ‘organization’</p> <p>A computer system component (e.g. DVD ROM drive, keyboard) Computer protocol(s), radio frequency(ies), subsystem(s),</p> <p>*Support*</p> <p>Budget</p>	<p>Resource</p> <p>a generalized service provided (often) by one party to another party</p>

Appendix 3 Data to Model Implementation Details

Named computer systems, named information technology, named satcom systems, named ,	Agent (with Agent Type attribute==it_system) – if it passes knowledge/information between other agents/organizations. Using computers imposes a cognitive load on people as well. Finally, intention is to model within construct the following: $p(\text{forgetting}) > 0 \ \& \ \ll 1$; $p(\text{! interact}) > 0 \ \& \ \ll 1$; $p(\text{tx err}) > 0 \ \& \ \ll 1$.
Computer network (jwics, NIPRNet, SIPRNet, *net) Unnamed/generic computer systems, generic references to technology, information technology, classes of IT systems (e.g., gps, dscs) Relay device(s) or nonmessage content manipulating device/capability (e.g., routers, switches, network) Switch, generic telephone, call manager(s), IT-enabled radars, weapons, radios,	Resource (with Resource Type attribute==it_resource)
Nonspecific position within orgs (e.g. officer, assistant secretary [without a qualifier]) Foe, Ally, adversary	Role
Management, process, reception, responsibilities, support, task, synchronize, plan, manage, establish, conduct,	Task
Acronyms ≤ 3 chars	Insert underscore between letters, look- up the definition and apply category based on definition Prefer to add deconstruction of acronym if feasible (e.g., <u>gps_global_positioning_system</u>)

Using frequency as culling decision input variable

At least for some measures, the heuristic of deleting nodes with low ‘frequency’ attributes will sabotage the use of the measure. Likewise the deleting of pendants, recursively or not, may inflict unexpected changes to the network.

Appendix 3 Data to Model Implementation Details

The D2M process, when generating the metanetwork, will generate several attributes per node in each of the node classes. One of those attributes is ‘Frequency,’ which is a simple count of how many times the concept (or its mapped-from predecessor) has appeared in the sets. This attribute does not, in isolation, provide a modeler with high confidence that the node(s) is worthy of deleting. I certainly ran across a number of instances when building these three models where the ‘frequency’ of a node was an order of magnitude lower than top nodes, yet other network measures revealed the node was relevant to the model for its position in the network structure as well as serving as a conduit from one node class to another.

In the specific case of the proposed static resilience measure, the measure requires the counting of near-isolated nodes in three node sets: agents; resources; and tasks. With the intuition that too many nearly isolated nodes leads to too many points of degraded access to people, resources, and tasks, it should be apparent to the reader that removing pendants necessarily decreases the number of nearly-isolated nodes. This is especially true for recursive deletion of pendant chains—where a chain of nodes is connected to nothing other than the next element of the chain.

Appendix 4 Virtual Experiment How-To Guide

This appendix repeats information from a research project that preceded the dissertation discussed elsewhere in this work. However, the methodology and practical how-to guide should benefit future researchers as well as those desiring to critique my work. This appendix describes exactly how the supporting infrastructure and the actual virtual experiments were carried out at a re-execution level of detail.

SVN or other Shared-work Repository

I've been using SVN as the code repository for all my work. I will write this recipe as if the reader will likewise be using SVN. I leave modifications and changes of the recipe to the reader if they using Git, CVS, SourceSafe, or some other technology/capability.

Create a named repository

I usually ask the SVN repository administrator to create a repository using some shortened version of the project name--if feasible. For example, if the project name is "Learned Multi-Level Resilience," I ask for a repository project called *multi-level*.

Checkout the named repository

Of course, a SVN client can checkout a project to a directory using the project's name or some arbitrary name. The choice is user specific and should be irrelevant to the remainder of this recipe.

Create a Directory Structure

Within the (presumably brand new and empty) project directory, create a directory structure. This structure is inherently specific to the researcher or the team of researchers. If a team, defining and settling on it early, though allowing modifications later, will make collaboration easier.

I have created several directory trees and depict them below starting at the project directory entitled multi-level. For the dissertation work, I replaced "multi-level" with "dissertation."

Appendix 4 Virtual Experiment How-To Guide

The two folders of immediate interest to the virtual experiment researcher are the *scriptsAndApps* folder and the *construct* folder. As depicted in [Figure 140](#), there are several sub-folders in the *scriptsAndApps* folder.

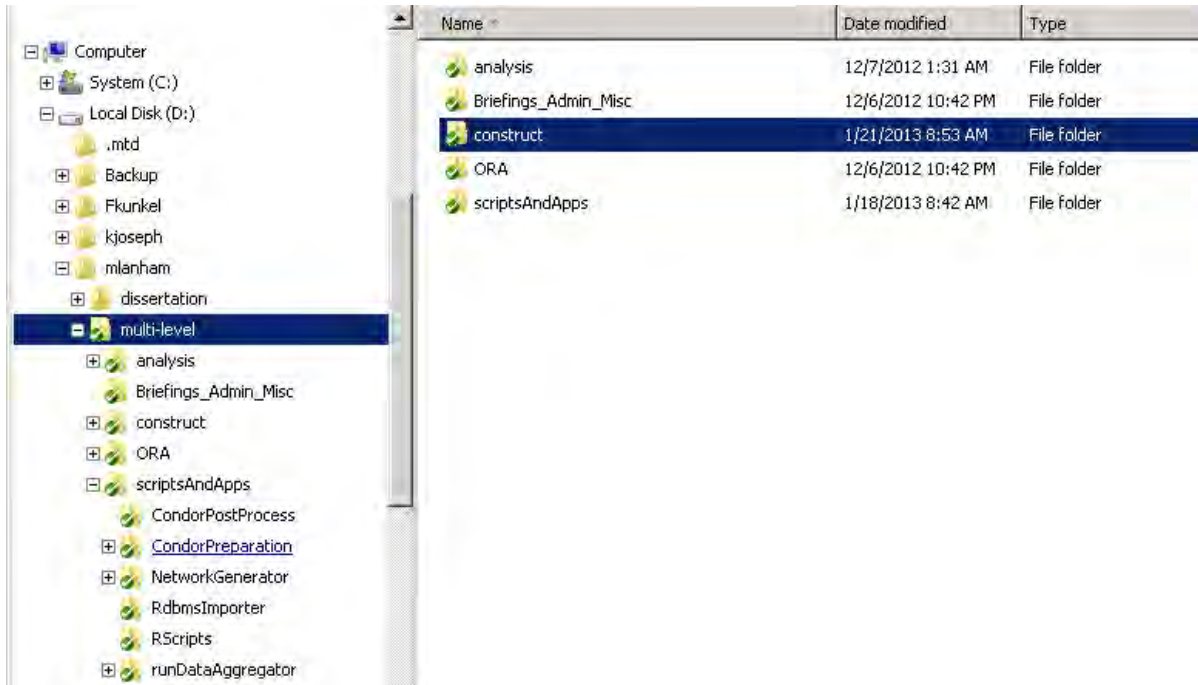


Figure 140: Directory structure for virtual experiments

Within the *construct* folder there are two folders, both required for the proper functioning of the automated scripts created for the learned multi-level resiliency project. The folders have the names *inputDecks* and *runs*. This tree is below in [Figure 141](#).

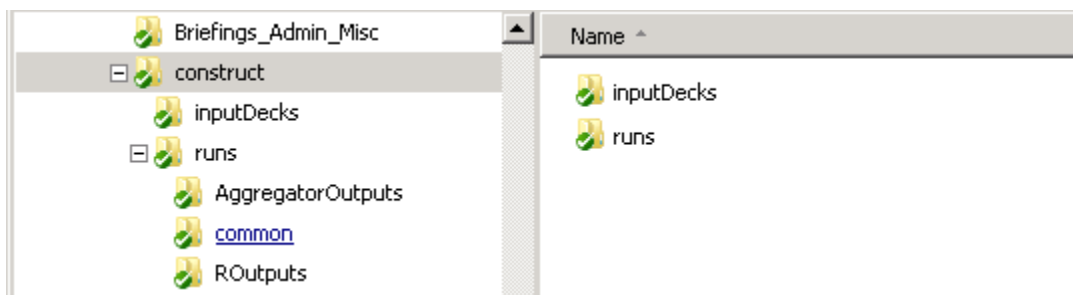


Figure 141: Directory structure for construct within virtual experiment directory structure

CondorPreparation - This folder is for the scripts and applications. Those scripts and applications pre-process inputs and write temporary outputs to disk. The folder also holds some helper scripts and .jar files used by the individual condor clients to help the researcher identify

problematic machines in the condor cluster. The .jar file is from the directory tree rooted in the *javaUtils* folder which is the root of an Eclipse IDE project.

NetworkGenerator - This folder is for the Java-based application to take the temporary outputs from the preparation scripts, generate construct networks, and write them to disk. It is the root of an Eclipse IDE project. The resultant exported executable jar is copied to a location I will discuss shortly.

CondorPostProcess - This folder holds several shell scripts (bash and perl) that help the researcher identify problems with the output from a condor run.

runDataAggregator - This folder is for the Java-based application to take the outputs of a construct run, conduct data reduction and processing enroute to information. It is the root of an Eclipse IDE project.

Input Files

The construct input deck can refer to one or more external files for loaded a simulation. The deck for the Multi-Level Project refers to a *params.csv* file that lists a number of key-value pairs. The reader will note *params.csv* **does not exist**, in the *inputDecks* folder. The pre-processing scripts automatically generate the *params.csv* from the *params_template.xls* file.

The *params_template.xls* file serves several functions

- It supports a single point of entry for variables (thereby reducing the probability of mis-typing parameters and/or their values elsewhere)
- It supports rapid and automatic generation of XML needed to define <var> elements in the input deck. *The Researcher may still need to copy the XML to the input deck manually.*
- It supports rapid and nearly automatic generation of XML relevant to defining <networks> or <operations> elements in the input deck. *The Researcher may still need to copy the XML to the input deck manually.*
- It supports the rapid and automatic generation of *params.csv* files unique to each configuration of the virtual experiment as well as the directory structure needed to isolate each of those configurations from the others.
- It supports the rapid and automatic data reduction, aggregation, and output of meaningful results by using the single point of entry for key-value pairs

Params_template.xls

This file, as of April 2013, needs to remain in the pre-Excel 2007 format of .xls.

Warning: Do not use the .xlsx format, as the perl script processing the file uses a CPAN module that does not support the .xlsx format.

The contents of params_template.xls are worth reviewing, column by column.

	A	B	C	D	E	F	G	H
1	Line	parameter	value	type	src	tgt	linktype	vars
2	0	a_attack_email_prob	0	float				value="readFromCSVFile[params.csv,0,construct::intvar::param_val_col]:float" />
3	1	a_attack_f2f_prob	0	float				<var name="a_attack_f2f_prob" value="readFromCSVFile[params.csv,1,construct::intvar::param_val_col]:float" />
4	2	a_attack_phone_prob	0	float				<var name="a_attack_phone_prob" value="readFromCSVFile[params.csv,2,construct::intvar::param_val_col]:float" />
5	3	a_attack_prob	0	float				<var name="a_attack_prob" value="readFromCSVFile[params.csv,3,construct::intvar::param_val_col]:float" />

Figure 142: Snapshot of params_template.xls, Columns A–H

Variables and their definitions

Column A should remain a zero-indexed list of integers, incremented by one (1) for each row. This information is needed in the XML in Column H to tell construct what row the variable definition resides on.

Column B is the variable's name. Construct does not allow spaces in variable names, nor to start with a numeric value. The example demonstrates an all lowercase style with words separated by underscores. As a matter of convention, I have maintained ascending alphabetical order for the variables in two groups: non-file name variables, and file name variables.

Column C is the value that the variable will assume in the *params.csv* file. The application that creates the directory structure for a virtual experiment as well as the data aggregator also uses the key-value pairs in Columns B & C.

Column D supports the generation of XML to define <var> elements in the input deck. Construct expects values to be “float”, “int”, “string”, and “bool.”

Column H is the XML definition of the <var> element that the *researcher needs to manually copy this entire column into the input deck*, overwriting the existing vars derived from *params_template.xls*.

WARNING: MS Excel copy and paste does not usually copy the MS-Excel escaped quotation marks in Column H into a text-only editor. A fast way to overcome this phenomena is to paste the material first into MS Word, then copy from MS Word the text to paste into the text-only editor.

Appendix 4 Virtual Experiment How-To Guide

Failure to copy and paste and ensure correct processing of escaped quotation marks may result in non-obvious deck failures!

Variables that impact <network> definitions

Columns E, F, and G store data needed to create a <network> element definition. A <network> is a collection of links between source and target nodes.

Column E is the type of node from which the link originates. It must be a value that construct expects and defined in the input deck's <nodes> tree. In the example, the src node type is shown as agent.

E	F	G	H	I	J
src	tgt	linktype	vars		networks
agent	agent	float	<code><var name="access_network_fname" value="readFromCSVFile[params.csv,62,construct::intvar:param_val_col]:string"/></code>		<pre> <!-- Load dichotomous access network from file --> <network src_nodeclass_type="agent" target_nodeclass_type="agent" id="access network" link_type="float" network_type="dense"> <generator type="csv"> <rows first="0" last="nodeclass::agent::count_minus_one"/> <cols first="0" last="nodeclass::agent::count_minus_one"/> <param name="filesystem_path" value="access_network_fname"/> <param name="skip_first_row" value="true"/> <param name="csvrow" value="construct::stringvar:agent_list"/> <param name="csvcol" value="construct::stringvar:agent_list"/> <param name="symmetric" value="true"/> <param name="load_style" value="sparse_to_dense_convert"/> <!-- <param name="subtract_one_from_indices" value="true"/> --> </generator> </pre>
agent	timeperiod	bool	<code><var name="agent_active_timeperiod_network_fname" value="readFromCSVFile[params.csv,63,construct::intvar:param_val_col]:string"/></code>		<pre> <!-- Load dichotomous agent active network from file --> <network src_nodeclass_type="agent" target_nodeclass_type="timeperiod" id="agent active timeperiod network" link_type="bool" network_type="dense"> <!-- default values --> <generator type="constant"> <rows first="0" last="nodeclass::agent::count_minus_one"/> <cols first="0" last="nodeclass::timeperiod::count_minus_one"/> <param name="constant_value" value="true"/> </generator> <!-- Load from File --> <generator type="csv_binimize"> <rows first="0" last="nodeclass::agent::count_minus_one"/> <cols first="0" last="nodeclass::timeperiod::count_minus_one"/> <param name="filesystem_path" value="agent_active_timeperiod_network_fname"/> <param name="skip_first_row" value="true"/> <param name="csvrow" value="construct::stringvar:agent_list"/> <param name="csvcol" value="construct::stringvar:timeperiod_list"/> <param name="load_style" value="sparse_to_dense_convert"/> <param name="binarization_threshold" value="0.0"/> <!-- <param name="subtract_one_from_indices" value="true"/> --> </generator> </network> </pre>

Figure 143: Snapshot params_templat.xls, Columns E-J

Column F is the type of node to which the link connects. It must be a value that construct expects and defined in the input deck's <nodes> tree. In the example, the tgt node type is an agent.

Column G is the link type. Construct expects this value to be one of the following: float, int, or bool. In the example, the linktype is a float in row 64 and bool in row 65.

Column H is, as discussed above for variables that do not impact network definitions, the XML definition of the <var> element. **The researcher needs to manually copy this entire column into the input deck.**

Column I is a visual separator and is not otherwise relevant.

Column J is a concatenation of Column K "Network Comment(s)" and Column L "additional network generators." This concatenation reduces the number of columns the researcher needs to manually copy, into the input deck while supporting the possibility of

Appendix 4 Virtual Experiment How-To Guide

multiple network generators per network definition. *The researcher needs to manually copy this entire column into the input deck, overwriting the existing <network> elements derived from params_template.xls.*

WARNING: MS Excel copy and paste does not usually copy the MS-Excel escaped quotation marks in Column H into a text-only editor. A fast way to overcome this phenomena is to paste the material first into MS Word, then copy from MS Word the text to paste into the text-only editor.

experiment_config_file.xls

This file, as of April 2013, needs to remain in the pre-Excel 2007 format of .xls.

Warning: Do not use the .xlsx format, as the perl script processing the file uses a CPAN module that does not support the .xlsx format.

This file is used by the makeCondorDirs script to setup the Box-Behnken experimental design. Each column represents a variable under test. The name of the variable must match exactly the variable name specified either in the deck or in the params_template.xls file. The second row is a comma-separated list of values that the variable can assume. Rows 3 and upwards (15 in the example above) are the values in the Box-Behnken design where -1 represents the lowest possible value from row 2, 0 represents the middle value from row 2, and 1 represents the highest value from row 2.

	A	B	C
1	c_attack_prob	i_attack_prob	a_attack_prob
2	0.0, 0.2, 0.8	0.0, 0.2, 0.8	0.0, 0.2, 0.8
3	-1	-1	0
4	-1	1	0
5	0	-1	-1
6	0	0	0
7	0	1	1
8	1	0	1
9	-1	0	1
10	1	0	-1
11	0	-1	1
12	1	1	0
13	0	1	-1
14	1	-1	0
15	-1	0	-1

Figure 144: Snapshot of experiment_config_file.xls

The *makeCondorDirs* script automatically reads and parses this file and applies its contents to the process of writing *params.csv* files for each of the experimental configurations under test.

The researcher must copy Columns H and J into the input deck if they have added or deleted any rows to the params_template.xls file. Failure to do update the input deck ensures the results will not reflect any changes to the template file!

Updating Executables sent to the Condor cluster

The submission of jobs to the Condor cluster includes passing multiple executable files to each Condor node. Each of these executables must be up-to-date before the researcher creates the directories for the virtual experiment and submitting the jobs to Condor for execution.

In the *scriptsAndApps* folder, the following files must be **current**:

- *construct.exe* - the agent-based simulation executable
- *networkGenerator.jar* - the executable jar that will, on the condor client, read the *params.csv* file, and generate the various input networks that construct needs to run. For the multi-level resilience project, this is a highly specific application though the division of labor between numerous applications may remain appropriate for other projects, such as this dissertation.

Appendix 4 Virtual Experiment How-To Guide

- *dataAggregator.jar* - the executable jar that will, on the submitting machine, recursively traverse, reduce, and process the outputs of the condor jobs. Each condor client will return the results of the run (as specified in the construct input deck) *and anything else* in the condor working directory of the client.

In the *CondorPreparation* folder, the following files must be **current**:

- *condorShell.cmd* - this MS DOS script (using the cmd.exe found on various flavors of MS Windows operating systems since Windows XP) is the application that the condor client executes directly. It performs a multi-step process on each client. A copy of the script I used is available on my personal web page at <http://www.andrew.cmu.edu/user/mlanham/dissertation/CondorPreparation/condorShell>.
 - Confirms Perl and Java are installed on the condor client
 - Confirms that Perl is installed (Cygwin Perl)
 - if Perl is not installed, the script sets a flag to cause the network generator application to failure over to Java alternatives to the Perl Scripts
 - Confirms that 64-bit java is installed
 - Makes a critical assumption that the 64-bit java.exe is in c:\program files\java since Microsoft uses the C:\Program Files (x86) directory as the default location for 32-bit applications on 32-bit machines.
 - If 64-bit java is not installed, the script fails with an errorcode set to 1.
 - Just before exiting, the script creates a file called `64_Bit_JAVA_IS_MISSING_ON_%HOST%` and replaces `%HOST%` with the name of the machine. This file gets returned to the submitting machine and a post-processing script can support a researcher's effort to identify and remediate machines without 64-bit java.
 - Note: 64-bit java has been necessary for several reasons
 - possibly sloppy coding that leads to heap and stack memory errors
 - insufficient heap and stack memory to process large quantities of large output files
 - Runs the *networkGenerator.jar* file
 - Run *construct* using *construct.xml* as the input
 - Deletes the input files and undesired output files.
 - Compresses the desired output files, then deletes the .csv versions
 - When the *condorShell.cmd* exits, the condor client transmits all the files in its working directory back to the submitting machine.
- *whichJVMIsInstalled.jar* - this Java application returns the highest version of installed JRE and JDK, if present, or an empty string if not present.

Perl on submitting machine

You must have Perl installed on the submitting machine to use the [makeCondorDirs.pl](#) PERL script. I've tested the scripts on cygwin perl 5.14.2. You must also have the following Perl

Appendix 4 Virtual Experiment How-To Guide

Packages installed (CPAN comes in handy for this). All are installed on zurg.CASOS.cs.cmu.edu, the machine The URL for the makeCondorDirs is

<http://www.andrew.cmu.edu/user/mlanham/dissertation/CondorPreparation/makeCondorDirs>.

- *File::Path* (v2.09 is the version I installed)
- *File::Copy::Recursive* (v0.38 is the version I have installed)
- *Getopt::Long* (v2.39 is the version I installed)
- *Getopt::Std* (v1.06 is the version I installed)
- *Switch* (v2.16 is the version I have installed)
- *Spreadsheet::ParseExcel* (v0.59 is the version I installed)

Directories for Condor Virtual Experiment

WARNING: The following steps need to be on a machine that can submit jobs to condor. If not, then the machine that can submit jobs to condor will need shared access to these folders and files to run.

The researcher should open a command prompt (cygwin is the shell prompt most used by the dissertation author) and change directory to the *runs* folder.

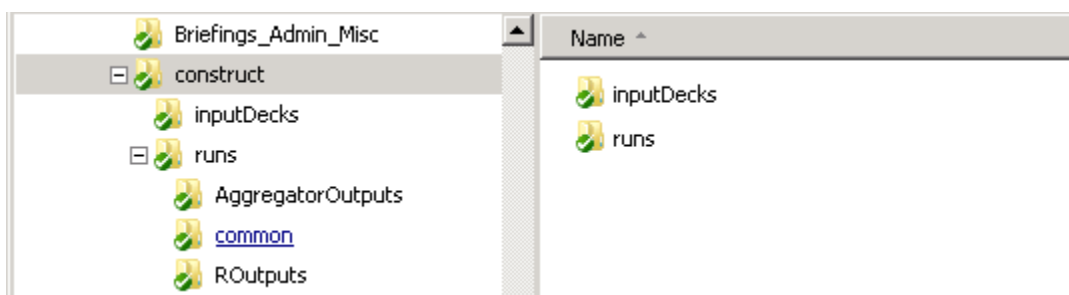


Figure 145: Directory structure for construct runs

Execute *makeCondorDirs.pl* script (which of course presumes the reader has Perl installed on their system). The specific invocation syntax is below:

```
../../scriptsAndApps/CondorPreparation/makeCondorDirs.pl --  
verbose -best -p ../../construct/inputDecks/params_template.xls  
-c ../../construct/inputDecks/experiment_config_file.xls -i  
../../construct/inputDecks/multiLevel_inputDeck.xml
```

makeCondorDirs.pl --help will show the options available for use as of April 2013.

Submitting to Condor for the Virtual Experiment

To submit to condor, assuming the condor client is installed and appropriately configured to submit to the condor cluster controller, enter the following command

Appendix 4 Virtual Experiment How-To Guide

```
condor_submit condor_submission_file0000.txt
```

Alternatively, you can setup a `for` loop such as the one

```
for i in `ls condor_submission_file00*`; do condor_submit $i;
done
```

The purpose of a five (5) minute delay between submissions is to allow some spacing of the file transmissions of the executables between the submitting client and the condor controller. It also spaces out the number of jobs on the controller at any given point. Finally, it spaces out the file transmissions from the executing condor client returning outputs to the submitting client.

Post-Processing Outputs of Condor from a Virtual Experiment

Data Aggregation

There are three ways to invoke the data aggregation. One is via an executable JAR file, the other is through Eclipse (assuming access to source code). The third is to have the aggregator run on the Condor Cluster. This recipe will review the running of the aggregator through Eclipse and then via the JAR file, and then the execution on the Condor Cluster.

Data Aggregation via Eclipse IDE

Assumption: The user has created a Java project within their Eclipse™ framework, and has the project correctly set to use Java 1.7 (there are reasons for using Java 1.7), `java-getopt-1.0.14.jar` as a Library in the Java Build Path.

Setup a *Run Configuration* using either the Run menu item or the drop down menu next to the run button as shown in the figure below.

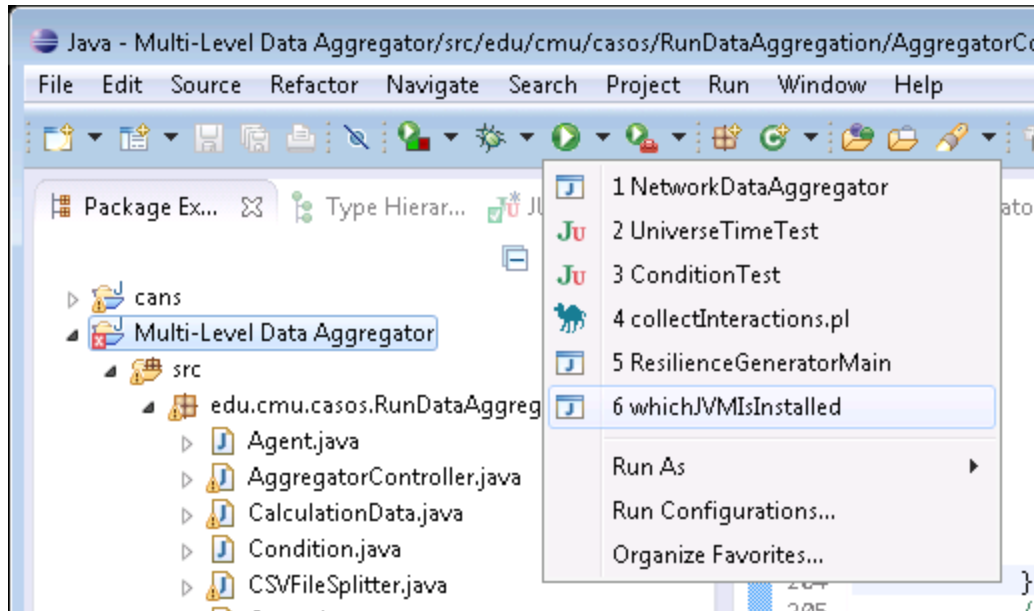


Figure 146: Eclipse's Run configurations menu item

After selecting *Run Configurations*, the model should create or edit the run configuration for the data aggregator. If creating, you'll want to click on the "Create Configuration" icon in the upper left corner, and if editing, you should see a window much like the one below. Ensure the Project name matches and the main class dialog box are correctly filled in.

You will also want to fill in the "Arguments" tab with the command line arguments as well as the working directory text box. The command line arguments are discussed below, and can be accessed using the command line execution environment with the -h option.

```
java -jar NetworkDataAggregator -h
Options, as of April 2013 are:
-f DirectoryName    Directories from Condor's virtual experiment
                    runs, naming convention has each starting
with
                    Condition_[int(s)]
-v                  verbose output
-d [ints >=1]      debug output of greater volume the higher the
int
-o DirectoryName    Directory where the Aggregator will write
output
                    files
```

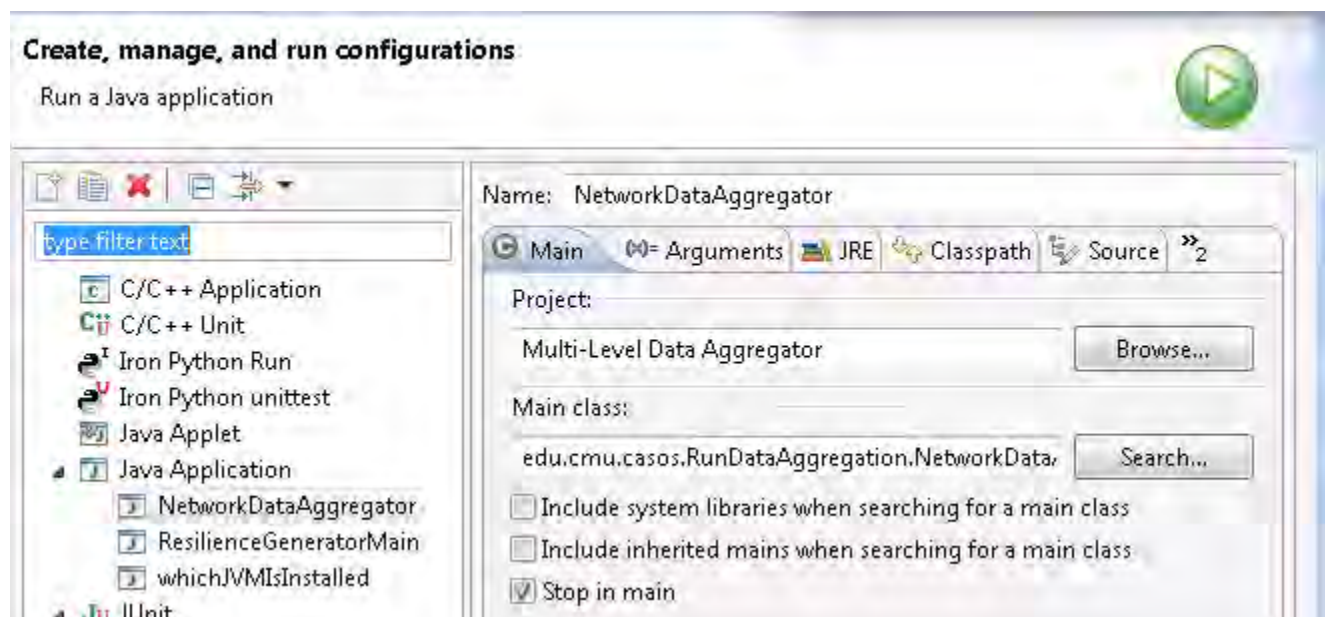


Figure 147: Eclipse run configuration for NetworkDataAggregator – main tab

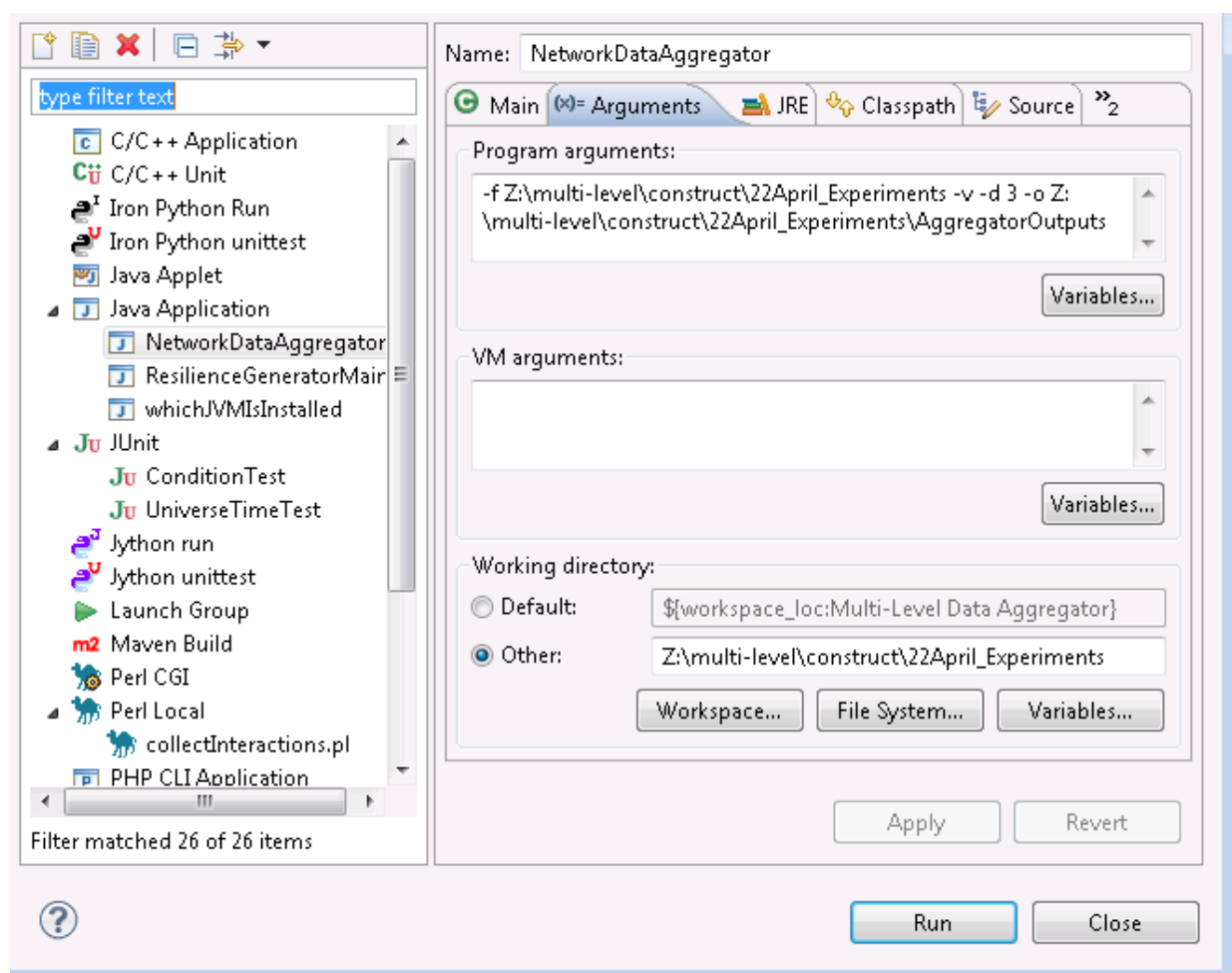


Figure 148: Eclipse run configuration for NetworkDataAggregator – arguments tab

Appendix 4 Virtual Experiment How-To Guide

The experimenter should also set the working directory to the same directory as the input directory. Once configured, the researcher can press “Apply” and “Close” and then invoke this run configuration at some future point in time.

Data Aggregator from the Command Line

Assuming the developer has exported a current and up-to-date copy of the executable JAR, the researcher can invoke it from the command line. For convenience, having the present working directory (pwd) as the input directory works well. The invocation is below:

```
java -jar NetworkDataAggregator -f inputDir [-v] [-d int] [-o outputDir]
```

If the output directory is not specified, the aggregator will write outputs to the present working directory.

Data Aggregation via Aggregator on Condor

Assuming the researcher has the outputs from the virtual experiment run available, aggregation on the Condor HPC is feasible.

The invocation for the Condor-based aggregator preparation program is shown below:

```
java -jar CondorBasedAggregator -f inputDir [-v] [-d int] [-o outputDir]
```

The outputs of this jar file will be a submission file per experimental condition as well as a series of .7z (7Zip) files that are the compressed outputs of the virtual experiment. The research may submit each condor submission file with an invocation like that shown below:

```
condor_submit condorBasedAggregation_0001.txt
```

Alternatively, you can setup a `for` loop such as the one shown below:

```
for i in `ls condorBasedAggregation_*`; do condor_submit $i; done
```

These condor jobs will transfer the compressed outputs of the virtual experiment directories. On the execute node, unzips the outputs, and processes the outputs. During processing it creates two (2) directories that Condor returns to the submitting node: AggregatorOutputs, and condition_00xx_AVG_Attributes.

Appendix 4 Virtual Experiment How-To Guide

To merge the results of these aggregator outputs into a single output file, use the bash script in the *CondorPostProcess* directory called *MergeAggregatorOutputs*. An example of invoking that shell script, from within the directory holding the results of the virtual experiment looks like this:

```
../../scriptsAndApps/CondorPostProcess/mergeAggregatorOutputs.sh
```

Using R for Graph Generation

Open R-Studio

Load “plotAllMetrics.r”

Change Line 4 “setwd” to match current run directory where aggregator data is stored

Change Line 8 if necessary

Change source lines 25 through 29 if necessary, which should be relative to the working directory

a. Set working dir in script if using IDE

Appendix 5 Construct Input Files

Parameters files

The table below is a listing of the parameter file used by the processing scripts and Construct. Electronic copies of the parameter file, the source code, and the executable jar file are available on my personal web page at

<http://www.andrew.cmu.edu/user/mlanham/dissertation/>

Table 62: Parameters used to in operational and strategic simulations

Line	Parameter	value
0	a_attack_email_prob	0
1	a_attack_key_it_prob	0
2	a_attack_phone_prob	0
3	a_attack_web_prob	0
4	agent_flip_to_negative_rate	0.1
5	agent_flip_to_positive_rate	0.1
6	attack_end_time	162
7	attack_start_time	50
8	c_attack_prob	0
9	email_preference_mean	0.2
10	email_preference_variance	0.02
11	facetoface_preference_mean	0.6
12	facetoface_preference_variance	0.06
13	group_flip_to_positive_rate	0.1
14	group_flip_to_negative_rate	0.1
15	human_agent_forgetting_mean	0.9

16	human_agent_forgetting_rate	0.01
17	human_agent_forgetting_variance	0
18	human_agent_initiation_count	2
19	human_agent_learn_by_doing	0.999
20	human_agent_message_complexity	5
21	human_agent_reception_count	1
22	human_agent_selective_attention	0.9999
23	i_attack_prob	0
24	it_agent_initiation_count	2
25	it_agent_forgetting_mean	0.54
26	it_agent_forgetting_rate	0.006
27	it_agent_forgetting_variance	0
28	it_agent_message_complexity	5
29	it_agent_reception_count	1
30	knowledge_count	3232
31	knowledge_general_count	2782
32	knowledge_plan_bad_count	150
33	knowledge_plan_count	300
34	knowledge_plan_priority	2
35	knowledge_priority	1
36	ktm_false_neg_rate	0.06
37	ktm_false_pos_rate	0.03
38	meeting_interaction_multiplier	9
39	meeting_plan_ratio	0.2
40	num_briefings	3
41	ora_input_fname	construct_ORA_file.xml
42	phone_preference_mean	0.1

Appendix 4 Virtual Experiment How-To Guide

43	phone_preference_variance	0.01
44	plan_briefing_1_end	57
45	plan_briefing_1_start	54
46	plan_briefing_2_end	75
47	plan_briefing_2_start	72
48	plan_briefing_3_end	93
49	plan_briefing_3_start	90
50	plan_briefing_duration	4
51	plan_briefing_interlude	14
52	plan_execution_ratio	0.3333
53	plan_time_count	53
54	social_proximity_weight	0.5
55	time_count	200
56	time_failover_complete	4

57	ttm_false_neg_rate	0.08
58	ttm_false_pos_rate	0.04
59	warm_up_period	40
60	warm_up_period_enabled	1
61	web_preference_mean	0.1
62	web_preference_variance	0.01
63	facetoface	0
64	phone_lvl1	1
65	phone_lvl2	2
66	email_lvl1	3
67	email_lvl2	4
68	web_lvl1	5
69	web_lvl2	6

Experimental Configuration File (Box-Behnken implementation)

The table below is the colorized experimental design file read by the Perl script to create directories, modify the parameters file shown above to reflect the experimentally varied values, and communicates the

Table 63: Box-Behnken design of six attack vectors and four mitigations

c_attack_prob	i_attack_prob	a_attack_key_it_prob	a_attack_email_prob	a_attack_phone_prob	a_attack_web_prob	ktm_false_pos_rate	ktm_false_neg_rate	ttm_false_pos_rate	ttm_false_neg_rate	time_failover_complete	meeting_plan_ratio
0.2,0.0,0.8	0.2,0.0,0.8	0.2,0.0,0.8	0.2,0.0,0.8	0.2,0.0,0.8	0.2,0.0,0.8	0.015,0.03,0.0075	0.02,0.04,0.01	0.03,0.015,0.06	0.04,0.02,0.08	1.0,0.0,3.0	0.40,0.20,0.6
0	-1	0	0	0	-1	-1	0	-1	0	0	-1
0	-1	0	0	0	-1	-1	0	-1	0	0	1
0	-1	0	0	0	-1	1	0	1	0	0	-1
0	-1	0	0	0	-1	1	0	1	0	0	1
0	-1	0	0	0	1	-1	0	-1	0	0	-1

Appendix 4 Virtual Experiment How-To Guide

c_attack_prob	i_attack_prob	a_attack_key_it_prob	a_attack_email_prob	a_attack_phone_prob	a_attack_web_prob	ktm_false_pos_rate	ktm_false_neg_rate	ttm_false_pos_rate	ttm_false_neg_rate	time_failover_complete	meeting_plan_ratio
0	-1	0	0	0	1	-1	0	-1	0	0	1
0	-1	0	0	0	1	1	0	1	0	0	-1
0	-1	0	0	0	1	1	0	1	0	0	1
0	1	0	0	0	-1	-1	0	-1	0	0	-1
0	1	0	0	0	-1	-1	0	-1	0	0	1
0	1	0	0	0	-1	1	0	1	0	0	-1
0	1	0	0	0	-1	1	0	1	0	0	1
0	1	0	0	0	1	-1	0	-1	0	0	-1
0	1	0	0	0	1	-1	0	-1	0	0	1
0	1	0	0	0	1	1	0	1	0	0	-1
0	1	0	0	0	1	1	0	1	0	0	1
-1	-1	0	0	-1	0	0	0	0	0	0	-1
-1	-1	0	0	-1	0	0	0	0	0	0	1
-1	-1	0	0	1	0	0	0	0	0	0	-1
-1	-1	0	0	1	0	0	0	0	0	0	1
-1	1	0	0	-1	0	0	0	0	0	0	-1
-1	1	0	0	-1	0	0	0	0	0	0	1
-1	1	0	0	1	0	0	0	0	0	0	-1
-1	1	0	0	1	0	0	0	0	0	0	1
1	-1	0	0	-1	0	0	0	0	0	0	-1
1	-1	0	0	-1	0	0	0	0	0	0	1
1	-1	0	0	1	0	0	0	0	0	0	-1
1	-1	0	0	1	0	0	0	0	0	0	1
1	1	0	0	-1	0	0	0	0	0	0	-1
1	1	0	0	-1	0	0	0	0	0	0	1
1	1	0	0	1	0	0	0	0	0	0	-1
1	1	0	0	1	0	0	0	0	0	0	1

Appendix 4 Virtual Experiment How-To Guide

c_attack_prob	i_attack_prob	a_attack_key_it_prob	a_attack_email_prob	a_attack_phone_prob	a_attack_web_prob	ktm_false_pos_rate	ktm_false_neg_rate	ttm_false_pos_rate	ttm_false_neg_rate	time_failover_complete	meeting_plan_ratio
0	-1	-1	0	0	0	-1	-1	-1	-1	0	0
0	-1	-1	0	0	0	-1	1	-1	1	0	0
0	-1	-1	0	0	0	1	-1	1	-1	0	0
0	-1	-1	0	0	0	1	1	1	1	0	0
0	-1	1	0	0	0	-1	-1	-1	-1	0	0
0	-1	1	0	0	0	-1	1	-1	1	0	0
0	-1	1	0	0	0	1	-1	1	-1	0	0
0	-1	1	0	0	0	1	1	1	1	0	0
0	1	-1	0	0	0	-1	-1	-1	-1	0	0
0	1	-1	0	0	0	-1	1	-1	1	0	0
0	1	-1	0	0	0	1	-1	1	-1	0	0
0	1	-1	0	0	0	1	1	1	1	0	0
0	1	1	0	0	0	-1	-1	-1	-1	0	0
0	1	1	0	0	0	-1	1	-1	1	0	0
0	1	1	0	0	0	1	-1	1	-1	0	0
0	1	1	0	0	0	1	1	1	1	0	0
0	-1	0	-1	0	-1	0	0	0	0	-1	0
0	-1	0	-1	0	-1	0	0	0	0	1	0
0	-1	0	-1	0	1	0	0	0	0	-1	0
0	-1	0	-1	0	1	0	0	0	0	1	0
0	-1	0	1	0	-1	0	0	0	0	-1	0
0	-1	0	1	0	-1	0	0	0	0	1	0
0	-1	0	1	0	1	0	0	0	0	-1	0
0	-1	0	1	0	1	0	0	0	0	1	0
0	1	0	-1	0	-1	0	0	0	0	-1	0
0	1	0	-1	0	-1	0	0	0	0	1	0
0	1	0	-1	0	1	0	0	0	0	-1	0

Appendix 4 Virtual Experiment How-To Guide

c_attack_prob	i_attack_prob	a_attack_key_it_prob	a_attack_email_prob	a_attack_phone_prob	a_attack_web_prob	ktm_false_pos_rate	ktm_false_neg_rate	ttn_false_pos_rate	ttn_false_neg_rate	time_failover_complete	meeting_plan_ratio
0	1	0	-1	0	1	0	0	0	0	1	0
0	1	0	1	0	-1	0	0	0	0	-1	0
0	1	0	1	0	-1	0	0	0	0	1	0
0	1	0	1	0	1	0	0	0	0	-1	0
0	1	0	1	0	1	0	0	0	0	1	0
-1	0	0	0	0	0	0	-1	0	-1	-1	-1
-1	0	0	0	0	0	0	-1	0	-1	-1	1
-1	0	0	0	0	0	0	-1	0	-1	1	-1
-1	0	0	0	0	0	0	-1	0	-1	1	1
-1	0	0	0	0	0	0	1	0	1	-1	-1
-1	0	0	0	0	0	0	1	0	1	-1	1
-1	0	0	0	0	0	0	1	0	1	1	-1
-1	0	0	0	0	0	0	1	0	1	1	1
1	0	0	0	0	0	0	-1	0	-1	-1	-1
1	0	0	0	0	0	0	-1	0	-1	-1	1
1	0	0	0	0	0	0	-1	0	-1	1	-1
1	0	0	0	0	0	0	-1	0	-1	1	1
1	0	0	0	0	0	0	1	0	1	-1	-1
1	0	0	0	0	0	0	1	0	1	-1	1
1	0	0	0	0	0	0	1	0	1	1	-1
1	0	0	0	0	0	0	1	0	1	1	1
0	0	-1	-1	-1	0	0	0	0	0	0	-1
0	0	-1	-1	-1	0	0	0	0	0	0	1
0	0	-1	-1	1	0	0	0	0	0	0	-1
0	0	-1	-1	1	0	0	0	0	0	0	1
0	0	-1	1	-1	0	0	0	0	0	0	-1
0	0	-1	1	-1	0	0	0	0	0	0	1

Appendix 4 Virtual Experiment How-To Guide

c_attack_prob	i_attack_prob	a_attack_key_it_prob	a_attack_email_prob	a_attack_phone_prob	a_attack_web_prob	ktm_false_pos_rate	ktm_false_neg_rate	ttn_false_pos_rate	ttn_false_neg_rate	time_failover_complete	meeting_plan_ratio
0	0	-1	1	1	0	0	0	0	0	0	-1
0	0	-1	1	1	0	0	0	0	0	0	1
0	0	1	-1	-1	0	0	0	0	0	0	-1
0	0	1	-1	-1	0	0	0	0	0	0	1
0	0	1	-1	1	0	0	0	0	0	0	-1
0	0	1	-1	1	0	0	0	0	0	0	1
0	0	1	1	-1	0	0	0	0	0	0	-1
0	0	1	1	-1	0	0	0	0	0	0	1
0	0	1	1	1	0	0	0	0	0	0	-1
0	0	1	1	1	0	0	0	0	0	0	1
-1	0	0	-1	0	0	-1	-1	-1	-1	0	0
-1	0	0	-1	0	0	-1	1	-1	1	0	0
-1	0	0	-1	0	0	1	-1	1	-1	0	0
-1	0	0	-1	0	0	1	1	1	1	0	0
-1	0	0	1	0	0	-1	-1	-1	-1	0	0
-1	0	0	1	0	0	-1	1	-1	1	0	0
-1	0	0	1	0	0	1	-1	1	-1	0	0
-1	0	0	1	0	0	1	1	1	1	0	0
1	0	0	-1	0	0	-1	-1	-1	-1	0	0
1	0	0	-1	0	0	-1	1	-1	1	0	0
1	0	0	-1	0	0	1	-1	1	-1	0	0
1	0	0	-1	0	0	1	1	1	1	0	0
1	0	0	1	0	0	-1	-1	-1	-1	0	0
1	0	0	1	0	0	-1	1	-1	1	0	0
1	0	0	1	0	0	1	-1	1	-1	0	0
1	0	0	1	0	0	1	1	1	1	0	0
0	0	-1	0	-1	0	-1	0	-1	0	-1	0

Appendix 4 Virtual Experiment How-To Guide

c_attack_prob	i_attack_prob	a_attack_key_it_prob	a_attack_email_prob	a_attack_phone_prob	a_attack_web_prob	ktm_false_pos_rate	ktm_false_neg_rate	ttm_false_pos_rate	ttm_false_neg_rate	time_failover_complete	meeting_plan_ratio
0	0	-1	0	-1	0	-1	0	-1	0	1	0
0	0	-1	0	-1	0	1	0	1	0	-1	0
0	0	-1	0	-1	0	1	0	1	0	1	0
0	0	-1	0	1	0	-1	0	-1	0	-1	0
0	0	-1	0	1	0	-1	0	-1	0	1	0
0	0	-1	0	1	0	1	0	1	0	-1	0
0	0	-1	0	1	0	1	0	1	0	1	0
0	0	1	0	-1	0	-1	0	-1	0	-1	0
0	0	1	0	-1	0	-1	0	-1	0	1	0
0	0	1	0	-1	0	1	0	1	0	-1	0
0	0	1	0	-1	0	1	0	1	0	1	0
0	0	1	0	1	0	-1	0	-1	0	-1	0
0	0	1	0	1	0	-1	0	-1	0	1	0
0	0	1	0	1	0	1	0	1	0	-1	0
0	0	1	0	1	0	1	0	1	0	1	0
-1	0	-1	0	0	-1	0	0	0	0	-1	0
-1	0	-1	0	0	-1	0	0	0	0	1	0
-1	0	-1	0	0	1	0	0	0	0	-1	0
-1	0	-1	0	0	1	0	0	0	0	1	0
-1	0	1	0	0	-1	0	0	0	0	-1	0
-1	0	1	0	0	-1	0	0	0	0	1	0
-1	0	1	0	0	1	0	0	0	0	-1	0
-1	0	1	0	0	1	0	0	0	0	1	0
1	0	-1	0	0	-1	0	0	0	0	-1	0
1	0	-1	0	0	-1	0	0	0	0	1	0
1	0	-1	0	0	1	0	0	0	0	-1	0
1	0	-1	0	0	1	0	0	0	0	1	0

Appendix 4 Virtual Experiment How-To Guide

c_attack_prob	i_attack_prob	a_attack_key_it_prob	a_attack_email_prob	a_attack_phone_prob	a_attack_web_prob	ktm_false_pos_rate	ktm_false_neg_rate	ttm_false_pos_rate	ttm_false_neg_rate	time_failover_complete	meeting_plan_ratio
1	0	1	0	0	-1	0	0	0	0	-1	0
1	0	1	0	0	-1	0	0	0	0	1	0
1	0	1	0	0	1	0	0	0	0	-1	0
1	0	1	0	0	1	0	0	0	0	1	0
0	0	0	-1	-1	-1	0	-1	0	-1	0	0
0	0	0	-1	-1	-1	0	1	0	1	0	0
0	0	0	-1	-1	1	0	-1	0	-1	0	0
0	0	0	-1	-1	1	0	1	0	1	0	0
0	0	0	-1	1	-1	0	-1	0	-1	0	0
0	0	0	-1	1	-1	0	1	0	1	0	0
0	0	0	-1	1	1	0	-1	0	-1	0	0
0	0	0	-1	1	1	0	1	0	1	0	0
0	0	0	1	-1	-1	0	-1	0	-1	0	0
0	0	0	1	-1	-1	0	1	0	1	0	0
0	0	0	1	-1	1	0	-1	0	-1	0	0
0	0	0	1	-1	1	0	1	0	1	0	0
0	0	0	1	1	-1	0	-1	0	-1	0	0
0	0	0	1	1	-1	0	1	0	1	0	0
0	0	0	1	1	1	0	-1	0	-1	0	0
0	0	0	1	1	1	0	1	0	1	0	0
0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0

Appendix 4 Virtual Experiment How-To Guide

c_attack_prob	i_attack_prob	a_attack_key_it_prob	a_attack_email_prob	a_attack_phone_prob	a_attack_web_prob	ktm_false_pos_rate	ktm_false_neg_rate	ttm_false_pos_rate	ttm_false_neg_rate	time_failover_complete	meeting_plan_ratio
0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0
1	1	1	0	0	0	0	0	0	0	0	0
0	0	0	1	1	1	0	0	0	0	0	0
1	1	1	1	1	1	0	0	0	0	0	0
1	1	1	1	1	1	1	1	1	1	1	0
1	1	1	1	1	1	-1	-1	-1	-1	-1	-1
1	1	1	1	1	1	-1	-1	0	0	0	0
1	1	1	1	1	1	0	0	-1	-1	1	1
1	1	1	1	1	1	0	0	0	0	-1	-1
0	0	1	0	0	0	0	0	0	0	-1	0
0	0	1	0	0	0	0	0	0	0	0	0
0	0	1	0	0	0	0	0	0	0	1	0
0	1	0	0	0	0	1	1	1	1	0	0
0	1	0	0	0	0	1	1	1	1	0	1

Appendix 6 Construct input deck for operational and strategic simulation

```
<construct>
<construct>
  <!-- ***** -->
>
  <!-- ***** GLOBAL VARIABLES ***** -->
  <!-- ***** -->
>
  <construct_vars>
    <!-- value is in col 1 (zero indexed) -->
    <var name="param_val_col" value="1" />
    <!-- ##### -->
    <!-- ##### -->
    <!-- ### Start vars from parameters file ### -->
    <!-- ### copy 60+ var xml nodes from params_template.xls Column H ## -->
    <!-- ### You may need to copy & paste into MS Word, then copy and ## -->
    <!-- ### paste into this XML document. It depends on how your ### -->
    <!-- ### XML editor handles the Excel-oddities of embedded ### -->
    <!-- ### quotations in a cell ### -->
    <!-- ##### -->
    <!-- ##### -->
    <var name="a_attack_email_prob"
value="readFromCSVFile[params.csv,0,construct::intvar::param_val_col]:float" />
    <var name="a_attack_key_it_prob"
value="readFromCSVFile[params.csv,1,construct::intvar::param_val_col]:float" />
    <var name="a_attack_phone_prob"
value="readFromCSVFile[params.csv,2,construct::intvar::param_val_col]:float" />
    <var name="a_attack_web_prob"
value="readFromCSVFile[params.csv,3,construct::intvar::param_val_col]:float" />
    <var name="agent_flip_to_negative_rate"
value="readFromCSVFile[params.csv,4,construct::intvar::param_val_col]:float" />
    <var name="agent_flip_to_positive_rate"
value="readFromCSVFile[params.csv,5,construct::intvar::param_val_col]:float" />
    <var name="attack_end_time"
value="readFromCSVFile[params.csv,6,construct::intvar::param_val_col]:int" />
    <var name="attack_start_time"
value="readFromCSVFile[params.csv,7,construct::intvar::param_val_col]:int" />
    <var name="c_attack_prob"
value="readFromCSVFile[params.csv,8,construct::intvar::param_val_col]:float" />
    <var name="email_preference_mean"
value="readFromCSVFile[params.csv,9,construct::intvar::param_val_col]:float" />
    <var name="email_preference_variance"
value="readFromCSVFile[params.csv,10,construct::intvar::param_val_col]:float" />
```

```
<var name="facetoface_preference_mean"
value="readFromCSVFile[params.csv,11,construct::intvar::param_val_col]:float" />
<var name="facetoface_preference_variance"
value="readFromCSVFile[params.csv,12,construct::intvar::param_val_col]:float" />
<var name="group_flip_to_positive_rate"
value="readFromCSVFile[params.csv,13,construct::intvar::param_val_col]:float" />
<var name="group_flip_to_negative_rate"
value="readFromCSVFile[params.csv,14,construct::intvar::param_val_col]:float" />
<var name="human_agent_forgetting_mean"
value="readFromCSVFile[params.csv,15,construct::intvar::param_val_col]:float" /><!-- for
use in binary forgetting -->
<var name="human_agent_forgetting_rate"
value="readFromCSVFile[params.csv,16,construct::intvar::param_val_col]:float" /><!-- for
use in non-binary forgetting -->
<var name="human_agent_forgetting_variance"
value="readFromCSVFile[params.csv,17,construct::intvar::param_val_col]:float" /><!-- for
use in binary forgetting -->
<var name="human_agent_initiation_count"
value="readFromCSVFile[params.csv,18,construct::intvar::param_val_col]:int" />
<var name="human_agent_learn_by_doing"
value="readFromCSVFile[params.csv,19,construct::intvar::param_val_col]:float" />
<var name="human_agent_message_complexity"
value="readFromCSVFile[params.csv,20,construct::intvar::param_val_col]:int" />
<var name="human_agent_reception_count"
value="readFromCSVFile[params.csv,21,construct::intvar::param_val_col]:int" />
<var name="human_agent_selective_attention"
value="readFromCSVFile[params.csv,22,construct::intvar::param_val_col]:float" />
<var name="i_attack_prob"
value="readFromCSVFile[params.csv,23,construct::intvar::param_val_col]:float" />
<var name="it_agent_initiation_count"
value="readFromCSVFile[params.csv,24,construct::intvar::param_val_col]:int" />
<var name="it_agent_forgetting_mean"
value="readFromCSVFile[params.csv,25,construct::intvar::param_val_col]:float" /><!-- for
use in binary forgetting -->
<var name="it_agent_forgetting_rate"
value="readFromCSVFile[params.csv,26,construct::intvar::param_val_col]:float" /><!-- for
use in non-binary forgetting -->
<var name="it_agent_forgetting_variance"
value="readFromCSVFile[params.csv,27,construct::intvar::param_val_col]:int" /><!-- for use
in binary forgetting -->
<var name="it_agent_message_complexity"
value="readFromCSVFile[params.csv,28,construct::intvar::param_val_col]:int" />
<var name="it_agent_reception_count"
value="readFromCSVFile[params.csv,29,construct::intvar::param_val_col]:int" />
```

Appendix 6 Construct input deck for operational and strategic simulation

```
<var name="knowledge_count"
value="readFromCSVFile[params.csv,30,construct::intvar::param_val_col]:int" /><!-- not
intended for use within the deck, used by params_template.xls to auto-calculate plan k and
bad-plan k size -->
<var name="knowledge_general_count"
value="readFromCSVFile[params.csv,31,construct::intvar::param_val_col]:int" /><!-- not
intended for use within the deck, used by params_template.xls to auto-calculate plan k and
bad-plan k size -->
<var name="knowledge_plan_bad_count"
value="readFromCSVFile[params.csv,32,construct::intvar::param_val_col]:int" /><!-- not
intended for use within the deck, auto-calculated by params_template.xls -->
<var name="knowledge_plan_count"
value="readFromCSVFile[params.csv,33,construct::intvar::param_val_col]:int" /><!-- not
intended for use within the deck, auto-calculated by params_template.xls -->
<var name="knowledge_plan_priority"
value="readFromCSVFile[params.csv,34,construct::intvar::param_val_col]:int" />
<var name="knowledge_priority"
value="readFromCSVFile[params.csv,35,construct::intvar::param_val_col]:int" />
<var name="ktm_false_neg_rate"
value="readFromCSVFile[params.csv,36,construct::intvar::param_val_col]:float" /><!--
replaced with agent/group flip rates for group-based TM generators -->
<var name="ktm_false_pos_rate"
value="readFromCSVFile[params.csv,37,construct::intvar::param_val_col]:float" /><!--
replaced with agent/group flip rates for group-based TM generators -->
<var name="meeting_interaction_multiplier"
value="readFromCSVFile[params.csv,38,construct::intvar::param_val_col]:int" />
<var name="meeting_plan_ratio"
value="readFromCSVFile[params.csv,39,construct::intvar::param_val_col]:float" />
<var name="num_briefings"
value="readFromCSVFile[params.csv,40,construct::intvar::param_val_col]:int" />
<var name="ora_input_fname"
value="readFromCSVFile[params.csv,41,construct::intvar::param_val_col]:string" />
<var name="phone_preference_mean"
value="readFromCSVFile[params.csv,42,construct::intvar::param_val_col]:float" />
<var name="phone_preference_variance"
value="readFromCSVFile[params.csv,43,construct::intvar::param_val_col]:float" />
<var name="plan_briefing_1_end"
value="readFromCSVFile[params.csv,44,construct::intvar::param_val_col]:int" />
<var name="plan_briefing_1_start"
value="readFromCSVFile[params.csv,45,construct::intvar::param_val_col]:int" />
<var name="plan_briefing_2_end"
value="readFromCSVFile[params.csv,46,construct::intvar::param_val_col]:int" />
<var name="plan_briefing_2_start"
value="readFromCSVFile[params.csv,47,construct::intvar::param_val_col]:int" />
<var name="plan_briefing_3_end"
value="readFromCSVFile[params.csv,48,construct::intvar::param_val_col]:int" />
```

```
<var name="plan_briefing_3_start"
value="readFromCSVFile[params.csv,49,construct::intvar::param_val_col]:int" />
<var name="plan_briefing_duration"
value="readFromCSVFile[params.csv,50,construct::intvar::param_val_col]:int" />
<var name="plan_briefing_interlude"
value="readFromCSVFile[params.csv,51,construct::intvar::param_val_col]:int" />
<var name="plan_execution_ratio"
value="readFromCSVFile[params.csv,52,construct::intvar::param_val_col]:float" />
<var name="plan_time_count"
value="readFromCSVFile[params.csv,53,construct::intvar::param_val_col]:int" />
<var name="social_proximity_weight"
value="readFromCSVFile[params.csv,54,construct::intvar::param_val_col]:float" />
<var name="time_count"
value="readFromCSVFile[params.csv,55,construct::intvar::param_val_col]:int" />
<var name="time_failover_complete"
value="readFromCSVFile[params.csv,56,construct::intvar::param_val_col]:int" />
<var name="ttm_false_neg_rate"
value="readFromCSVFile[params.csv,57,construct::intvar::param_val_col]:float" /><!--
replaced with agent/group flip rates for group-based TM generators -->
<var name="ttm_false_pos_rate"
value="readFromCSVFile[params.csv,58,construct::intvar::param_val_col]:float" /><!--
replaced with agent/group flip rates for group-based TM generators -->
<var name="warm_up_period"
value="readFromCSVFile[params.csv,59,construct::intvar::param_val_col]:int" />
<var name="warm_up_period_enabled"
value="readFromCSVFile[params.csv,60,construct::intvar::param_val_col]:int" />
<var name="web_preference_mean"
value="readFromCSVFile[params.csv,61,construct::intvar::param_val_col]:float" />
<var name="web_preference_variance"
value="readFromCSVFile[params.csv,62,construct::intvar::param_val_col]:float" />
<var name="facetoface"
value="readFromCSVFile[params.csv,63,construct::intvar::param_val_col]:int" />
<var name="phone_lv11"
value="readFromCSVFile[params.csv,64,construct::intvar::param_val_col]:int" />
<var name="phone_lv12"
value="readFromCSVFile[params.csv,65,construct::intvar::param_val_col]:int" />
<var name="email_lv11"
value="readFromCSVFile[params.csv,66,construct::intvar::param_val_col]:int" />
<var name="email_lv12"
value="readFromCSVFile[params.csv,67,construct::intvar::param_val_col]:int" />
<var name="web_lv11"
value="readFromCSVFile[params.csv,68,construct::intvar::param_val_col]:int" />
<var name="web_lv12"
value="readFromCSVFile[params.csv,69,construct::intvar::param_val_col]:int" />
```

Appendix 6 Construct input deck for operational and strategic simulation

```
<!-- deck calculated value instead of always checking the numerous
vars that would indicate an attack: attack end time > 0; *_attack_*_prob > 0
used to include attack start time > 0, but there could be use cases where attacks start at
time 0 -->
<var name="attack_enabled" value="
  if((construct::floatvar::a_attack_email_prob > 0)
    || (construct::floatvar::a_attack_key_it_prob > 0)
    || (construct::floatvar::a_attack_phone_prob > 0)
    || (construct::floatvar::a_attack_web_prob > 0)
    || (construct::floatvar::c_attack_prob > 0)
    || (construct::floatvar::i_attack_prob > 0)
    || (construct::floatvar::a_attack_key_it_prob > 0)){
    true
  } else {
    false
  }
"/>
<!-- ##### end copy vars from parameters file ##### -->
<var name="attack_time_list"
value="construct::intvar::attack_start_time..construct::intvar::attack_end_time" />
<var name="attack_time_list_plus_one"
value="construct::stringvar::attack_time_list,(construct::intvar::attack_end_time+1) " />
<var name="attacktime_output_list" value="
  if (construct::boolvar::attack_enabled) {
    (construct::intvar::attack_start_time-1)..(construct::intvar::attack_end_time+1)
  } else {
    0
  }
"/>
<var name="belief_count" value="0" />
<var name="CommunicationMedium_list"
value="construct::intvar::facetoface..construct::intvar::web_lvl2" />
<var name="dummy_nodeclass_list" value="0" /> <!-- eases use of params_template.xls-
->
<var name="energytask_count" value="0" />
<var name="timeperiod_list" value="0..(construct::intvar::time_count - 1) " /> <!-- out of
alpha-order, but I need it now -->
<var name="plan_meeting_ticks" value="0..(construct::intvar::plan_briefing_duration-
1)" />
<var name="planning_timeperiod_list" value="(construct::intvar::warm_up_period +
1)..(construct::intvar::warm_up_period + construct::intvar::plan_time_count)" />
<var name="meeting_id_list" value="if (construct::intvar::num_briefings > 0) {
  0..(construct::intvar::num_briefings-1)
} else {
  0
}" />
```

```
<var name="output_by_percentiles" value="
  $currTime$ = 0;
  $step$ = construct::intvar::time_count / 10; /* 10% step value, ASSUMES time_count
>= 10 so $step$ >= (int)1 */
  $result$ = " + $currTime$;
  foreach $i$ (timeperiod_list){
    if ($i::int == ($currTime$ + $step$) ){
      $result$ = $result$ + ',' + ($currTime$ + $step$);
      $currTime$ = $i::int;
    } else {
      $currTime$ = $currTime$; /* non-harm else statement, since 'else' is not optional in
Construct's 'if then else' statements */
    }
  }
  /* now add the last time period to the list */
  $result$ = $result$ + ',' + (construct::intvar::time_count - 1);
  return $result$;
  with="$result$" />
<var name="plan_briefing_time_list" value="

  $plan_briefing_1_time_list$=construct::intvar::plan_briefing_1_start..construct::intvar::pla
n_briefing_1_end;

  $plan_briefing_2_time_list$=construct::intvar::plan_briefing_2_start..construct::intvar::pla
n_briefing_2_end;

  $plan_briefing_3_time_list$=construct::intvar::plan_briefing_3_start..construct::intvar::pla
n_briefing_3_end;
  $result$ = $plan_briefing_1_time_list$ + ',' + $plan_briefing_2_time_list$ + ',' +
$plan_briefing_3_time_list$;
  return $result$;
  with="$result$" />
</construct_vars>
<!-- *****
>
<!-- ***** GLOBAL SIMULATION PARAMETERS
***** -->
<!-- *****
>
<construct_parameters>
  <!-- set to 1 for testing to ensure consistent output
  @WARNING comment the line below for runs for record -->
  <!-- <param name="seed" value="1.0" />
  --> <param name="verbose_initialization" value="true" />
  <param name="verbose_verification" value="true" />
```

Appendix 6 Construct input deck for operational and strategic simulation

```
<param name="verbose_output_timing" value="false" />
<param name="verbose_interaction_weights" value="false" />
<param name="active_models" value="standard interaction model,standard task model"
with="delay_interpolation" />
<param name="active_mechanisms" value="none" />
<param name="belief_model" value="disable" />
<param name="binary_forgetting" value="true" />
<param name="communicationWeightForBelief" value="0.0" />
<param name="communicationWeightForBeliefTM" value="0.0" />

<param name="communicationWeightForFact" value="0.6" />
<param name="communicationWeightForKnowledgeTM" value="0.4" />

<param name="communicationWeightForBinaryTaskAssignment" value="0.0" />
<param name="communicationWeightForBinaryTaskAssignmentTM" value="0.1" />
<!-- <param name="operation_output_working_directory"
value="":c:/Users/Michael.Lanham/Google_Drive/dissertation/construct/strategic"/>
-->
<param name="default_agent_type" value="human" />
<param name="dynamic_environment" value="false" />
<param name="forgetting" value="true" />
<param name="interaction_requirements" value="disable" />
<param name="thread_count" value="1" />

<param name="transactive_memory" value="enable"/> <!-- other option is enable |
disable-->
<param name="tm_model" value="multi_level"/> <!-- multi_level | full_tm -->
<param name="activation_threshold_agent" value="-1" /> <!-- used in TM enabled in
multi_level mode, optional, default=-1 -->
<param name="activation_threshold_group" value="-2" /> <!-- used in TM enabled in
multi_level mode, optional, default=-1 -->
<param name="agent_annealing_halflife" value="6" /> <!-- used in TM enabled in
multi_level mode, optional, default=6 -->
<param name="group_annealing_halflife" value="6" /> <!-- used in TM enabled in
multi_level mode, optional, default=6 -->

<param name="use_mail" value="false" />

</construct_parameters>
<!--
#####
##### -->
<!--
#####
##### -->
```

```
<!-- ##### Start groups' names and node IDs from parameters file
##### -->
<!-- ##### copy 30+ xml nodes from params_template.xlsx Sheet 'GroupNames'
Column C ##### -->
<!-- ##### You may need to copy & paste into MS Word, then copy and paste # -
-->
<!-- ##### into this XML document. It depends on how your XML editor handles
## -->
<!-- ##### the Excel-oddities of embedded quotations in a cell
##### -->
<!--
#####
##### -->
<!--
#####
##### -->
<nodes>
  <!-- mandatory non-empty nodeclass read from Strategic model DynetML file-->
  <nodeclass type="agent" id="agent"> <!-- id serves as the prefix to the counter for node
IDs -->
    <properties>
      <property name="generate_nodeclass" value="true" />
      <property name="generator_type" value="dynetml"/>
      <property name="generator_doc_path"
value="construct::stringvar::ora_input_fname" />
      <property name="generator_nodeclass_id" value="agent" />
      <property name="generator_nodeclass_type" value="agent" />
    </properties>
  </nodeclass>
  <!-- mandatory non-empty nodeclass read from Strategic model DynetML files, uses
organization node set-->
  <nodeclass type="agentgroup" id="agentgroup">
    <properties>
      <property name="generate_nodeclass" value="true" />
      <property name="verbose" value="true" />
      <property name="generator_type" value="dynetml"/>
      <property name="generator_doc_path"
value="construct::stringvar::ora_input_fname" />
      <property name="generator_nodeclass_id" value="organization" />
      <property name="generator_nodeclass_type" value="Organization" />
    </properties>
  </nodeclass>
  <nodeclass type="agent_type" id="agent_type">
    <node id="human" title="human">
      <properties>
        <property name="communicationMechanism" value="direct" />
```

Appendix 6 Construct input deck for operational and strategic simulation

```
<property name="canSendCommunication" value="true" />
<property name="canReceiveCommunication" value="true" />
<property name="canSendKnowledge" value="true" />
<property name="canReceiveKnowledge" value="true" />
<property name="canSendKnowledgeTM" value="true" />
<property name="canReceiveKnowledgeTM" value="true" />
<property name="canSendReferral" value="true" />
<property name="canReceiveReferral" value="true" />
<property name="canSendBinaryTaskAssignmentTM" value="true"/>
<property name="canReceiveBinaryTaskAssignmentTM" value="true"/>
<property name="canSendBinaryTaskAssignment" value="false"/> <!--
assignment of tasks not part of lanham's dissertation -->
<property name="canReceiveBinaryTaskAssignment" value="false"/> <!--
assignment of tasks not part of lanham's dissertation -->
<property name="canSendBeliefs" value="false" /> <!-- beliefs not part of
lanham's dissertation -->
<property name="canReceiveBeliefs" value="false" /> <!-- beliefs not part of
lanham's dissertation -->
<property name="canSendBeliefsTM" value="false" /> <!-- beliefs not part of
lanham's dissertation -->
<property name="canReceiveBeliefsTM" value="false" /> <!-- beliefs not part of
lanham's dissertation -->
</properties>
</node>
<node id="it" title="it">
<properties>
<property name="communicationMechanism" value="direct" />
<property name="canSendCommunication" value="true" />
<property name="canReceiveCommunication" value="true" />
<property name="canSendKnowledge" value="true" />
<property name="canReceiveKnowledge" value="true" />
<property name="canSendBeliefs" value="false" />
<property name="canReceiveBeliefs" value="false" />
<property name="canSendBeliefsTM" value="false" />
<property name="canReceiveBeliefsTM" value="false" />
<property name="canSendBinaryTaskAssignmentTM" value="false"/>
<property name="canReceiveBinaryTaskAssignmentTM" value="false"/>
<property name="canSendBinaryTaskAssignment" value="false"/> <!--
assignment of tasks not part of lanham's dissertation -->
<property name="canReceiveBinaryTaskAssignment" value="false"/> <!--
assignment of tasks not part of lanham's dissertation -->
<property name="canSendKnowledgeTM" value="false" />
<property name="canReceiveKnowledgeTM" value="false" />
<property name="canSendReferral" value="true" />
<property name="canReceiveReferral" value="true" />
</properties>
```

```
</node>
</nodeclass>
<nodeclass type="CommunicationMedium" id="CommunicationMedium">
<properties>
<property name="generate_nodeclass" value="true" />
<property name="verbose" value="true" />
<property name="generator_type" value="dynetml"/>
<property name="generator_doc_path"
value="construct::stringvar::ora_input_fname" />
<property name="generator_nodeclass_id" value="comms_media" />
<property name="generator_nodeclass_type" value="Resource" />
</properties>
</nodeclass>
<nodeclass type="knowledge" id="knowledge">
<properties>
<property name="generate_nodeclass" value="true" />
<property name="generator_type" value="dynetml"/>
<property name="generator_doc_path"
value="construct::stringvar::ora_input_fname" />
<property name="generator_nodeclass_id" value="knowledge" />
<property name="generator_nodeclass_type" value="knowledge" />
</properties>
</nodeclass>
<nodeclass type="knowledgegroup" id="knowledgegroup">
<properties>
<property name="generate_nodeclass" value="true" />
<property name="generator_type" value="dynetml"/>
<property name="generator_doc_path"
value="construct::stringvar::ora_input_fname" />
<property name="generator_nodeclass_id" value="knowledgegroup" />
<property name="generator_nodeclass_type" value="unknown" />
</properties>
</nodeclass>
<nodeclass type="binarytask" id="binarytask">
<properties>
<property name="generate_nodeclass" value="true" />
<property name="generator_type" value="dynetml"/>
<property name="generator_doc_path"
value="construct::stringvar::ora_input_fname" />
<property name="generator_nodeclass_id" value="task" />
<property name="generator_nodeclass_type" value="task" />
</properties>
</nodeclass>
<nodeclass type="timeperiod" id="timeperiod">
<properties>
```

Appendix 6 Construct input deck for operational and strategic simulation

```
<property name="generate_nodeclass" value="true" />
<property name="generator_type" value="count" />
<property name="generator_count" value="construct::intvar::time_count" />
</properties>
</nodeclass>
<nodeclass type="dummy_nodeclass" id="dummy_nodeclass">
  <node id="constant" title="constant" />
</nodeclass>
</nodes>

<networks>
  <!-- need these first two grouping networks defined early, as they are used in a lot of the
  generators -->
  <network src_nodeclass_type="agent" target_nodeclass_type="agentgroup" id="agent
  group membership network" link_type="bool" network_type="dense">
    <!-- need to assign agents to one or more groups within the simulation -->
    <!-- Load from File -->
    <generator type="dynetml">
      <param name="filesystem_path" value="construct::stringvar::ora_input_fname" />
      <param name="network_name" value="agent x organization" />
      <param name="transpose" value="false" /> <!-- transpose after reading? optional
  param, default = false -->
      <rows first="0" last="nodeclass::agent::count_minus_one" />
      <cols first="0" last="nodeclass::agentgroup::count_minus_one" />
      <param name="verbose" value="false" />
    </generator>
  </network>
  <network src_nodeclass_type="knowledge" target_nodeclass_type="knowledgegroup"
  id="knowledge group membership network" link_type="bool" network_type="dense">
    <generator type="dynetml">
      <!-- @warning note the use of single quotes to force construct to treat
      the 'value' as an entire string, else the : and \ cause the Construct lexer fits ! -->
      <param name="filesystem_path" value="construct::stringvar::ora_input_fname" />
      <param name="network_name" value="knowledge x knowledgegroup" />
      <param name="transpose" value="false" /> <!-- transpose after reading? optional
  param, default = false -->
      <rows first="0" last="nodeclass::knowledge::count_minus_one" />
      <cols first="0" last="nodeclass::knowledgegroup::count_minus_one" />
      <param name="verbose" value="false" />
    </generator>
  </network>

  <!-- *****
  remainder of networks are in alphabetical order by network name/id
  *****-->
```

```
<network src_nodeclass_type="agent" target_nodeclass_type="agent" id="access
network" link_type="float" network_type="dense">
  <generator type="dynetml">
    <!-- read agent x agent access network from ORA file -->
    <param name="filesystem_path" value="construct::stringvar::ora_input_fname" />
    <param name="network_name" value="agent x agent" />
    <param name="transpose" value="false" /> <!-- transpose after reading? optional
  param, default = false -->
    <rows first="0" last="nodeclass::agent::count_minus_one" />
    <cols first="0" last="nodeclass::agent::count_minus_one" />
  </generator>
  <generator type="randombinary">
    <!-- connect level 1 key IT agents to the confidentiality sink with probability
  c_attack_prob -->
    <rows groups="it_agent_key_level1_group" group_membership_network="agent
  group membership network" />
    <cols groups="confidentiality_sink_group" group_membership_network="agent
  group membership network" />
    <param name="mean" value="construct::floatvar::c_attack_prob" />
  </generator>
  <generator type="randombinary">
    <!-- connect level 1 integrity agent to level 1 key IT Agents with probability
  i_attack_prob -->
    <rows groups="integrity_agent_level1_group" group_membership_network="agent
  group membership network" />
    <cols groups="it_agent_key_level1_group" group_membership_network="agent
  group membership network" />
    <param name="mean" value="construct::floatvar::i_attack_prob" />
  </generator>
  <generator type="randombinary">
    <!-- connect level 2 integrity agent to level 2 Key IT Agents with probability
  i_attack_prob -->
    <rows groups="integrity_agent_level2_group" group_membership_network="agent
  group membership network" />
    <cols groups="it_agent_key_level2_group" group_membership_network="agent
  group membership network" />
    <param name="mean" value="construct::floatvar::i_attack_prob" />
    <!--<param name="density" value="0.05" />--> <!-- for use with erdos_renyi -->
  </generator>
</network>
  <network src_nodeclass_type="agent" target_nodeclass_type="timeperiod" id="agent
  active timeperiod network" link_type="bool" network_type="dense"> <!--default values -->
    <generator type="constant"><!-- turn all agents on at all times -->
      <rows groups="all_agent_group" group_membership_network="agent group
  membership network" />
      <cols first="0" last="nodeclass::timeperiod::count_minus_one" />
```


Appendix 6 Construct input deck for operational and strategic simulation

```

    <param name="constant_value" value="1.0" />
  </generator>
  <generator type="constant"><!-- turn off integrity and confidentiality agents by default
-->
    <rows groups="integrity_agent_group, confidentiality_sink_group"
group_membership_network="agent group membership network" />
    <cols values="all" />
    <param name="constant_value" value="0" />
  </generator>
  <generator type="constant"><!-- turn off jopes as the source of plan knowledge until
the start of the planning period-->
    <rows values="426,434" />
    <cols values="construct::intvar::warm_up_period" />
    <param name="constant_value" value="0" />
  </generator>
  <generator type="randombinary"><!-- turn integrity agent on at specified probability
during 'attack' times -->
    <!-- during attacks, integrity agents get turned on, key agents get turned off, and spare
agents get turned on-->
    <rows groups="integrity_agent_group" group_membership_network="agent group
membership network" />
    <cols values="attack_time_list" />
    <param name="mean" value="if (construct::boolvar::attack_enabled) {
construct::floatvar::i_attack_prob
} else {
0.0
}" />
  </generator>
  <generator type="randombinary"><!-- if attacks enabled, turned off 80% is the same as
turned on 20%, else on all the time-->
    <rows groups="it_agent_key_level1_group, it_agent_key_level2_group"
group_membership_network="agent group membership network" />
    <cols values="attack_time_list" />
    <param name="mean" value="if (construct::boolvar::attack_enabled) {
1.0 - construct::floatvar::a_attack_key_it_prob
} else {
1.0
}" />
  </generator>
  <generator type="randombinary"><!-- when confidentiality attacks are enabled, turn
the sink(s) on probabilistically for the entire run -->
    <rows groups="confidentiality_sink_group" group_membership_network="agent
group membership network" />
    <cols values="0..nodeclass::timeperiod::count_minus_one" />
    <param name="mean" value="if (construct::floatvar::c_attack_prob > 0.0) {
construct::floatvar::c_attack_prob } else {

```

```

0
}" />
  </generator>
  <generator type="constant">
    <!-- if an availability Key IT attack is 'on', turn spare key IT on with specified delay
(time_failover_complete) as an integer multiplier of a (plan + brief) cycle,
once turned on during an attack, spare IT systems stay on until end of simulation --
>
    <rows
groups="it_agent_key_level1_spare_group, it_agent_key_level2_spare_group"
group_membership_network="agent group membership network" />
    <cols values="
$spares_on$ = '0';
if (construct::intvar::a_attack_key_it_prob > 0.0) {
$spares_on$ = (construct::intvar::attack_start_time
+ (construct::intvar::time_failover_complete
* (construct::intvar::plan_briefing_duration +
construct::intvar::plan_briefing_interlude))).nodeclass::timeperiod::count_minus_one;
} else {
$spares_on$ = '0';
}
return $spares_on$;" />
    <param name="constant_value" value="1.0" />
  </generator>
</network>
<network src_nodeclass_type="agent" target_nodeclass_type="timeperiod" id="agent
alive timeperiod network" link_type="bool" network_type="dense">
  <generator type="constant">
    <!-- mark all agents 'alive' at all times -->
    <rows first="0" last="nodeclass::agent::count_minus_one" />
    <cols first="0" last="nodeclass::timeperiod::count_minus_one" />
    <param name="constant_value" value="1.0" />
  </generator>
  <generator type="constant">
    <!-- make confidentiality agents 'alive' if c_attack is enabled-->
    <rows groups="confidentiality_sink_group" group_membership_network="agent
group membership network" />
    <cols first="0" last="nodeclass::timeperiod::count_minus_one" />
    <param name="constant_value" value="if (construct::floatvar::c_attack_prob > 0.0)
{
1.0
} else {
0.0
}
" />
  </generator>

```

Appendix 6 Construct input deck for operational and strategic simulation

```
<generator type="constant">
  <!-- make integrity agents 'alive' if i_attack is enabled-->
  <rows groups="integrity_agent_group" group_membership_network="agent group
membership network" />
  <cols first="0" last="nodeclass::timeperiod::count_minus_one" />
  <param name="constant_value" value="if (construct::floatvar::i_attack_prob > 0.0){
    1.0
  } else {
    0.0
  }
  " />
</generator>
</network>
<network src_nodeclass_type="agent" target_nodeclass_type="timeperiod" id="agent
initiation count network" link_type="int" network_type="dense">
  <!-- Assign number of initiations per turn per agent -->
  <generator type="constant">
    <!--default values for all human agents -->
    <rows groups="human_agent_group" group_membership_network="agent group
membership network" />
    <cols first="0" last="nodeclass::timeperiod::count_minus_one" />
    <param name="constant_value"
value="construct::intvar::human_agent_initiation_count" />
  </generator>
  <generator type="constant">
    <!--default values for all it agents -->
    <rows groups="it_agent_group" group_membership_network="agent group
membership network" />
    <cols first="0" last="nodeclass::timeperiod::count_minus_one" />
    <param name="constant_value" value="construct::intvar::it_agent_initiation_count"
/>
  </generator>
  <generator type="constant">
    <!-- confidentiality agent is a sink, and does not initiate interactions but does receive
interactions -->
    <rows groups="confidentiality_sink_group" group_membership_network="agent
group membership network" />
    <cols first="0" last="nodeclass::timeperiod::count_minus_one" />
    <param name="constant_value" value="0" />
  </generator>
  <generator type="constant">
    <!-- JPG planners get to talk more throughout the planning period -->
    <rows groups="jpg_joint_planning_group" group_membership_network="agent
group membership network" />
    <cols values="construct::stringvar::planning_timeperiod_list" />
  </generator>
</network>
```

```
<param name="constant_value"
value="construct::intvar::human_agent_initiation_count *
construct::intvar::meeting_interaction_multiplier" />
</generator>
<generator type="constant">
  <!-- JPG briefing attendees get to talk more throughout the briefing periods -->
  <rows groups="jpg_briefing" group_membership_network="agent group
membership network" />
  <cols values="construct::intvar::plan_briefing_time_list" />
  <param name="constant_value"
value="construct::intvar::human_agent_initiation_count *
construct::intvar::meeting_interaction_multiplier" />
</generator>
</network>
<network src_nodeclass_type="agent" target_nodeclass_type="timeperiod" id="agent
message complexity network" link_type="int" network_type="dense">
  <!-- Assign default complexity of messages per agent per time period -->
  <generator type="constant">
    <!-- Assign humans and integrity agents default human complexity -->
    <rows groups="human_agent_group, integrity_agent_group"
group_membership_network="agent group membership network" />
    <cols first="0" last="nodeclass::timeperiod::count_minus_one" />
    <param name="constant_value"
value="construct::intvar::human_agent_message_complexity" />
  </generator>
  <generator type="constant">
    <!-- assign IT systems default IT Systems message complexity, which is
(presumably) more complex messages -->
    <rows groups="it_agent_group" group_membership_network="agent group
membership network" />
    <cols first="0" last="nodeclass::timeperiod::count_minus_one" />
    <param name="constant_value"
value="construct::intvar::it_agent_message_complexity" />
  </generator>
</network>
<network src_nodeclass_type="agent" target_nodeclass_type="timeperiod" id="agent
reception count network" link_type="int" network_type="dense">
  <!-- Assign number of receptions per turn per agent -->
  <generator type="constant">
    <!--default values for all human agents -->
    <rows groups="human_agent_group" group_membership_network="agent group
membership network" />
    <cols first="0" last="nodeclass::timeperiod::count_minus_one" />
    <param name="constant_value"
value="construct::intvar::human_agent_reception_count" />
  </generator>
</network>
```

Appendix 6 Construct input deck for operational and strategic simulation

```

<generator type="constant">
  <!-- default values for all it agents -->
  <rows groups="it_agent_group" group_membership_network="agent group
membership network" />
  <cols first="0" last="nodeclass::timeperiod::count_minus_one" />
  <param name="constant_value" value="construct::intvar::it_agent_reception_count"
/>
</generator>
<generator type="constant">
  <!-- JPG planners get to listen more throughout the planning period -->
  <rows groups="jpg_joint_planning_group" group_membership_network="agent
group membership network" />
  <cols values="construct::intvar::planning_timeperiod_list" />
  <param name="constant_value"
value="construct::intvar::human_agent_initiation_count *
construct::intvar::meeting_interaction_multiplier" />
</generator>
<generator type="constant">
  <!-- JPG briefing attendees in meetings get to listen more -->
  <rows groups="jpg_briefing" group_membership_network="agent group
membership network" />
  <cols values="construct::intvar::planning_timeperiod_list" />
  <param name="constant_value"
value="construct::intvar::human_agent_reception_count *
construct::intvar::meeting_interaction_multiplier" />
</generator>
<generator type="constant">
  <!-- integrity agents don't listen to anybody -->
  <rows groups="integrity_agent_group" group_membership_network="agent group
membership network" />
  <cols first="0" last="nodeclass::timeperiod::count_minus_one" />
  <param name="constant_value" value="0" />
</generator>
</network>
<network src_nodeclass_type="agent" target_nodeclass_type="knowledge" id="agent
forgetting rate network" link_type="float" network_type="dense">
  <!-- set per agent per knowledge forgetting rates when non-binary forgetting is
enabled
  @todo for Mike Lanham's dissertation, execute an excursion where this network is
zero'ed out
  to see if construct really does only use this for non-binary forgetting -->
  <generator type="constant">
    <!-- set default forgetting rate for humans -->
    <rows groups="human_agent_group" group_membership_network="agent group
membership network" />
    <cols first="0" last="nodeclass::knowledge::count_minus_one" />

```

```

    <param name="constant_value"
value="construct::floatvar::human_agent_forgetting_rate"/>
    <!--
      <param name="min" value="if ((construct::floatvar::human_agent_forgetting_rate-
(3.0*construct::floatvar::human_agent_forgetting_variance)) < 0.0) {0.0} else
{construct::floatvar::human_agent_forgetting_rate-
(3.0*construct::floatvar::human_agent_forgetting_variance)}"/>
      <param name="max" value="if
(((construct::floatvar::human_agent_forgetting_rate+(3.0*construct::floatvar::human_agent_for
getting_variance)) > 1.0) {1.0} else
{construct::floatvar::human_agent_forgetting_rate+(3.0*construct::floatvar::human_agent_for
getting_variance)}"/>
    -->
    <param name="symmetric_flag" value="false"/>
  </generator>
  <generator type="constant">
    <!-- set default forgetting rate for humans -->
    <rows groups="human_agent_group" group_membership_network="agent group
membership network" />
    <cols groups="plan_k,bad_plan_k" group_membership_network="knowledge
group membership network" />
    <param name="constant_value" value="2 *
construct::floatvar::human_agent_forgetting_rate"/>
    <param name="symmetric_flag" value="false"/>
  </generator>
  <generator type="constant">
    <!-- set default forgetting rate for IT systems (including confidentiality agent),
which is 0.6 of default human rate -->
    <rows groups="it_agent_group" group_membership_network="agent group
membership network" />
    <cols first="0" last="nodeclass::knowledge::count_minus_one"/>
    <param name="constant_value"
value="construct::floatvar::human_agent_forgetting_variance"/>
    <!--
      <param name="min" value="if
((((construct::floatvar::human_agent_forgetting_rate*0.6)-
(3.0*construct::floatvar::human_agent_forgetting_variance)) < 0.0) {0.0} else
{construct::floatvar::human_agent_forgetting_rate*0.6)-
(3.0*construct::floatvar::human_agent_forgetting_variance)}"/>
      <param name="max" value="if
((((construct::floatvar::human_agent_forgetting_rate*0.6)+(3.0*construct::floatvar::human_age
nt_forgetting_variance)) > 1.0) {1.0} else
{construct::floatvar::human_agent_forgetting_rate*0.6)+(3.0*construct::floatvar::human_age
nt_forgetting_variance)}"/>
    -->
    <param name="symmetric_flag" value="false"/>
  </generator>
  <generator type="constant">
    <!-- set default forgetting rate for humans -->

```

Appendix 6 Construct input deck for operational and strategic simulation

```

<rows groups="it_agent_group" group_membership_network="agent group
membership network" />
<cols groups="plan_k,bad_plan_k" group_membership_network="knowledge
group membership network" />
<param name="constant_value" value="2 *
construct::floatvar::human_agent_forgetting_rate"/>
<param name="symmetric_flag" value="false"/>
</generator>
<generator type="randomuniform">
<!-- set default forgetting rate for all agents' bad plan' knowledge, 1.5 * regular
knowledge ,
including confidentiality agents-->
<rows first="0" last="nodeclass::agent::count_minus_one"/>
<cols groups="bad_plan_k" group_membership_network="knowledge group
membership network" />
<param name="max" value="if
(((construct::floatvar::human_agent_forgetting_rate*1.5)+(3.0*construct::floatvar::human_age
nt_forgetting_variance)) > 1.0) {1.0} else
{(construct::floatvar::human_agent_forgetting_rate*1.5)+(3.0*construct::floatvar::human_age
nt_forgetting_variance)}"/>
<param name="min" value="
if (((construct::floatvar::human_agent_forgetting_rate*1.5)-
(3.0*construct::floatvar::human_agent_forgetting_variance)) < 0.0) {
0.0
} else {
if (((construct::floatvar::human_agent_forgetting_rate*1.5)-
(3.0*construct::floatvar::human_agent_forgetting_variance)) > 1.0) {
0.99
} else {
(construct::floatvar::human_agent_forgetting_rate*1.5)-
(3.0*construct::floatvar::human_agent_forgetting_variance)
}
}
"/>
<param name="symmetric_flag" value="false"/>
</generator>
<generator type="constant">
<!-- set default integrity system forgetting rate for 'bad plan' knowledge==0 -->
<rows groups="integrity_agent_group" group_membership_network="agent group
membership network" />
<cols groups="bad_plan_k" group_membership_network="knowledge group
membership network" />
<param name="constant_value" value="0.0"/>
</generator>
</network>

```

```

<network src_nodeclass_type="agent" target_nodeclass_type="dummy_nodeclass"
id="agent forgetting mean network" link_type="float" network_type="dense">
<!-- set per agent forgetting mean when binary forgetting is enabled, its the probability
the bit will be completely forgot-->
<generator type="randomnormal">
<!-- set the general human agent forgetting rate-->
<rows groups="human_agent_group" group_membership_network="agent group
membership network" />
<cols first="0" last="0"/>
<param name="mean"
value="construct::floatvar::human_agent_forgetting_mean"/>
<param name="variance"
value="construct::floatvar::human_agent_forgetting_variance"/>
<param name="symmetric_flag" value="false"/>
</generator>
<generator type="constant">
<!-- set the it agent forgetting rate to 0.6 of human forgetting rate-->
<rows groups="human_agent_group" group_membership_network="agent group
membership network" />
<cols first="0" last="0"/>
<param name="constant_value"
value="construct::floatvar::human_agent_forgetting_mean * 0.6"/>
<param name="symmetric_flag" value="false"/>
</generator>
<generator type="constant">
<!-- set the integrity agent forgetting rate to 0 -->
<rows groups="integrity_agent_group" group_membership_network="agent group
membership network" />
<cols first="0" last="0"/>
<param name="constant_value" value="0" />
<param name="symmetric_flag" value="false"/>
</generator>
</network>
<network src_nodeclass_type="agent" target_nodeclass_type="dummy_nodeclass"
id="agent forgetting variance network" link_type="float" network_type="dense">
<!-- set per agent forgetting variance when binary forgetting is enabled-->
<generator type="constant">
<rows first="0" last="nodeclass::agent::count_minus_one"/>
<cols first="0" last="0"/>
<param name="constant_value"
value="construct::floatvar::human_agent_forgetting_variance"/>
<param name="symmetric_flag" value="false"/>
</generator>
</network>
<network src_nodeclass_type="agent" target_nodeclass_type="dummy_nodeclass"
id="agent learn by doing rate network" link_type="float" network_type="dense">

```

Appendix 6 Construct input deck for operational and strategic simulation

```
<generator type="randomuniform">
  <rows first="0" last="nodeclass::agent::count_minus_one"/>
  <cols first="0" last="0"/>
  <param name="min" value="1.0-
construct::floatvar::human_agent_learn_by_doing"/>
  <param name="max" value="construct::floatvar::human_agent_learn_by_doing"/>
  <param name="symmetric_flag" value="false"/>
</generator>
</network>
<network src_nodeclass_type="agent" target_nodeclass_type="knowledge" id="agent
learning rate network" link_type="float" network_type="dense">
  <generator type="constant">
    <rows first="0" last="nodeclass::agent::count_minus_one"/>
    <cols first="0" last="nodeclass::knowledge::count_minus_one"/>
    <param name="constant_value"
value="construct::floatvar::human_agent_learn_by_doing"/>
    <param name="symmetric_flag" value="false"/>
  </generator>
</network>
<network src_nodeclass_type="agent" target_nodeclass_type="dummy_nodeclass"
id="agent selective attention effect network" link_type="float" network_type="dense">
  <generator type="constant">
    <rows first="0" last="nodeclass::agent::count_minus_one" />
    <cols first="0" last="nodeclass::dummy_nodeclass::count_minus_one" />
    <param name="constant_value" value="1.0" /><!-- agent considers all known bits
eligible to send -->
  </generator>
</network>
<network src_nodeclass_type="agent" target_nodeclass_type="dummy_nodeclass"
id="agent type name network" link_type="string" network_type="dense">
  <generator type="constant">
    <rows groups="human_agent_group" group_membership_network="agent group
membership network" />
    <cols first="0" last="nodeclass::dummy_nodeclass::count-1"/>
    <param name="constant_value" value="human"/>
  </generator>
  <generator type="constant">
    <rows groups="it_agent_group" group_membership_network="agent group
membership network" />
    <cols first="0" last="nodeclass::dummy_nodeclass::count-1"/>
    <param name="constant_value" value="it"/>
  </generator>
</network>
<network src_nodeclass_type="agent" target_nodeclass_type="binarytask"
id="binarytask assignment network" link_type="bool" network_type="dense">
  <generator type="dynetml">
```

```
    <param name="filesystem_path" value="construct::stringvar::ora_input_fname" />
    <param name="network_name" value="agent x task" />
    <param name="transpose" value="false" /> <!-- transpose after reading? optional
param, default = false -->
    <rows first="0" last="nodeclass::agent::count_minus_one" />
    <cols first="0" last="nodeclass::binarytask::count_minus_one" />
    <param name="verbose" value="false"/>
  </generator>
</network>
<network src_nodeclass_type="knowledge" target_nodeclass_type="binarytask"
id="binarytask requirement network" link_type="bool" network_type="dense">
  <generator type="dynetml">
    <param name="filesystem_path" value="construct::stringvar::ora_input_fname" />
    <param name="network_name" value="knowledge x task" />
    <param name="transpose" value="false" /> <!-- transpose after reading? optional
param, default = false -->
    <rows first="0" last="nodeclass::agent::count_minus_one" />
    <cols first="0" last="nodeclass::binarytask::count_minus_one" />
    <param name="verbose" value="false" />
  </generator>
</network>
<network src_nodeclass_type="agent" target_nodeclass_type="timeperiod"
id="binarytask similarity weight network" link_type="float" network_type="dense">
  <!-- random values for human agent in the absence of empirical data -->
  <generator type="randomnormal">
    <rows groups="human_agent_group" group_membership_network="agent group
membership network" />
    <cols first="0" last="nodeclass::timeperiod::count_minus_one" />
    <param name="mean" value="0.6" />
    <param name="variance" value="0.06" />
  </generator>
  <!-- very low but non-zero random values for it agents in the absence of empirical data
-->
  <generator type="randomnormal">
    <rows groups="it_agent_group" group_membership_network="agent group
membership network" />
    <cols first="0" last="nodeclass::timeperiod::count_minus_one" />
    <param name="mean" value="0.01" />
    <param name="variance" value="0.05" />
  </generator>
</network>
<network src_nodeclass_type="knowledge" target_nodeclass_type="binarytask"
id="binarytask truth network" link_type="bool" network_type="dense">
  <generator type="dynetml">
    <param name="filesystem_path" value="construct::stringvar::ora_input_fname" />
    <param name="network_name" value="knowledge x task" />
```

Appendix 6 Construct input deck for operational and strategic simulation

```
<param name="transpose" value="false" /> <!-- transpose after reading? optional
param, default = false -->
<rows first="0" last="nodeclass::agent::count_minus_one" />
<cols first="0" last="nodeclass::binarytask::count_minus_one" />
</generator>
</network>
<network src_nodeclass_type="agent" target_nodeclass_type="CommunicationMedium"
id="communication medium access network" link_type="float" network_type="dense">
  <!-- Agent access to one or more communications mediums. Without access to >= 1,
the agent cannot communicate with anyone -->
  <!-- Load from File -->
  <generator type="dynetml">
    <param name="filesystem_path" value="construct::stringvar::ora_input_fname" />
    <param name="network_name" value="agent x comms_media" />
    <param name="transpose" value="false" />
    <rows first="0" last="nodeclass::agent::count_minus_one" />
    <cols first="0" last="nodeclass::CommunicationMedium::count_minus_one" />
  </generator>
</network>
<network src_nodeclass_type="agent" inner_nodeclass_type="agent"
target_nodeclass_type="CommunicationMedium" id="communication medium preferences
network 3d" link_type="float" network_type="dense3d">
  <!-- As a 3D network, cannot read in from ORA, so must create it within construct-->
  <generator type="constant3d">
    <!-- IT systems on level 1 can only use web to talk with other level 1 systems and
humans -->
    <rows groups="it_agent_level1_group" group_membership_network="agent
group membership network" />
    <inners groups="it_agent_level1_group,human_agent_group"
group_membership_network="agent group membership network" />
    <cols values="web_lv11" />
    <param name="constant_value" value="1.0" />
  <!--
  <param name="verbose" value="true" /> -->
  </generator>
  <generator type="constant3d">
    <!-- web interaction is the only choice to interact with IT systems as the target/alter-
->
    <rows groups="human_agent_group" group_membership_network="agent group
membership network" />
    <inners groups="it_agent_level1_group" group_membership_network="agent
group membership network" />
    <cols values="web_lv11" />
    <param name="constant_value" value="1.0" />
  </generator>
  <generator type="constant3d">
    <!-- IT systems on level 2 can only use web to talk with other level 2 systems -->
```

```
<rows groups="it_agent_level2_group" group_membership_network="agent group
membership network" />
  <inners groups="it_agent_level2_group,human_agent_level2_group"
group_membership_network="agent group membership network" />
  <cols values="web_lv12" />
  <param name="constant_value" value="1.0" />
<!--
  <param name="verbose" value="true" /> -->
</generator>
<generator type="constant3d">
  <rows groups="human_agent_level2_group" group_membership_network="agent
group membership network" />
  <inners groups="it_agent_level2_group" group_membership_network="agent
group membership network" />
  <cols values="web_lv12" />
  <param name="constant_value" value="1.0" />
<!--
  <param name="verbose" value="true" /> -->
</generator>
<generator type="constant3d">
  <!-- human agents prefer face-to-face with each other X% of the time -->
  <!-- @TODO fix this so its collocation, non-collocation sensitive -->
  <!-- @TODO add randomUniform3d as a generator type -->
  <rows groups="human_agent_group" group_membership_network="agent group
membership network" />
  <inners groups="human_agent_group" group_membership_network="agent group
membership network" />
  <cols values="facetoface" />
  <param name="constant_value"
value="construct::floatvar::facetoface_preference_mean" />
</generator>
<generator type="constantdiagonal3d">
  <!-- human agents when talking to themselves are assured of access via facetoface--
>
  <rows groups="human_agent_group" group_membership_network="agent group
membership network" />
  <inners groups="human_agent_group" group_membership_network="agent group
membership network" />
  <cols values="facetoface" />
  <param name="constant_value" value="1.0" />
</generator>
<generator type="constant3d">
  <!-- human agents prefer phone & email (unfiltered & filtered) with each other Y%
of the time, respectively -->
  <!-- @TODO fix this so its collocation, non-collocation sensitive -->
  <rows groups="human_agent_group" group_membership_network="agent group
membership network" />
```

Appendix 6 Construct input deck for operational and strategic simulation

```
<inners groups="human_agent_group" group_membership_network="agent group
membership network" />
<cols values="phone_lv11" />
<param name="constant_value"
value="construct::floatvar::phone_preference_mean" />
<!-- <param name="verbose" value="true" /> -->
</generator>
<generator type="constant3d">
<rows groups="human_agent_level2_group" group_membership_network="agent
group membership network" />
<inners groups="human_agent_level2_group" group_membership_network="agent
group membership network" />
<cols values="phone_lv12" />
<param name="constant_value"
value="construct::floatvar::phone_preference_mean" />
<!-- <param name="verbose" value="true" /> -->
</generator>
<generator type="constant3d">
<rows groups="human_agent_group" group_membership_network="agent group
membership network" />
<inners groups="human_agent_group" group_membership_network="agent group
membership network" />
<cols values="email_lv11" />
<param name="constant_value"
value="construct::floatvar::email_preference_mean" />
<!-- <param name="verbose" value="true" /> -->
</generator>
<generator type="constant3d">
<rows groups="human_agent_level2_group" group_membership_network="agent
group membership network" />
<inners groups="human_agent_level2_group" group_membership_network="agent
group membership network" />
<cols values="email_lv12" />
<param name="constant_value"
value="construct::floatvar::email_preference_mean" />
<!-- <param name="verbose" value="true" /> -->
</generator>
<generator type="constant3d">
<!-- human agents prefer web (unfiltered & filtered) with each other Z% of the time,
respectively -->
<!-- @TODO fix this so its collocation, non-collocation sensitive -->
<rows groups="human_agent_group" group_membership_network="agent group
membership network" />
<inners groups="human_agent_group" group_membership_network="agent group
membership network" />
<cols values="web_lv11" />
```

```
<param name="constant_value" value="construct::floatvar::web_preference_mean"
/>
<!-- <param name="verbose" value="true" /> -->
</generator>
<generator type="constant3d">
<rows groups="human_agent_level2_group" group_membership_network="agent
group membership network" />
<inners groups="human_agent_level2_group" group_membership_network="agent
group membership network" />
<cols values="web_lv12" />
<param name="constant_value" value="construct::floatvar::web_preference_mean"
/>
<!-- <param name="verbose" value="true" /> -->
</generator>
</network>
<network src_nodeclass_type="agent" target_nodeclass_type="knowledge"
id="interaction knowledge weight network" link_type="float" network_type="dense">
<!-- for each agent, weight the ego places on the specific knowledge bits when picking
an interaction partner -->
<generator type="constant"><!-- default values -->
<!-- start off with all agents (human and IT) weighting all knowledge equally -->
<rows first="0" last="nodeclass::agent::count_minus_one" />
<cols first="0" last="nodeclass::knowledge::count_minus_one" />
<param name="constant_value" value="construct::intvar::knowledge_priority" />
</generator>
<generator type="constant"><!-- plan knowledge is equally valued by all -->
<rows first="0" last="nodeclass::agent::count_minus_one" />
<cols groups="plan_k,bad_plan_k" group_membership_network="knowledge
group membership network" />
<param name="constant_value" value="construct::intvar::knowledge_plan_priority"
/>
</generator>
</network>
<network src_nodeclass_type="agent" target_nodeclass_type="agent" id="interaction
sphere network" link_type="bool" network_type="dense">
<!-- starting absolute agent x agent interaction network -->
<generator type="dynetml">
<param name="filesystem_path" value="construct::stringvar::ora_input_fname" />
<param name="network_name" value="agent x agent" />
<param name="transpose" value="false" /> <!-- transpose after reading? optional
param, default = false -->
<rows first="0" last="nodeclass::agent::count_minus_one" />
<cols first="0" last="nodeclass::agent::count_minus_one" />
</generator>
</network>
```

Appendix 6 Construct input deck for operational and strategic simulation

```
<network src_nodeclass_type="agent" target_nodeclass_type="timeperiod"
id="knowledge expertise weight network" link_type="float" network_type="dense">
  <!-- weight each ego gives to knowledge bits it does not have when deciding which
alter to interact with -->
  <!--default values -->
  <generator type="randomuniform">
    <rows first="0" last="nodeclass::agent::count_minus_one" />
    <cols first="0" last="nodeclass::timeperiod::count_minus_one" />
    <param name="min" value="0.4" />
    <param name="max" value="0.9" />
  </generator>
  <generator type="randomuniform">
    <!-- during briefings, jpg briefing attendees like to get knowledge they don't have --
>
    <rows groups="jpg_briefing" group_membership_network="agent group
membership network" />
    <cols values="construct::stringvar::planning_timeperiod_list" />
    <param name="min" value="0.8" />
    <param name="max" value="0.9999" />
  </generator>
  <generator type="randomuniform">
    <!-- during planning, jpg planners like to get knowledge they don't have -->
    <rows groups="jpg_joint_planning_group" group_membership_network="agent
group membership network" />
    <cols values="construct::stringvar::plan_briefing_time_list" />
    <param name="min" value="0.8" />
    <param name="max" value="0.9999" />
  </generator>
  <generator type="constant">
    <!-- integrity agents are interested in spreading bad knowledge, they weight agents
without bad plan knowledge more heavily than other agents -->
    <rows groups="integrity_agent_group" group_membership_network="agent group
membership network" />
    <cols values="construct::stringvar::plan_briefing_time_list" />
    <param name="constant_value" value="0.9999" />
  </generator>
</network>
<network src_nodeclass_type="agent" target_nodeclass_type="knowledge"
id="knowledge network" link_type="float" network_type="dense">
  <!-- agent x knowledge assignment -->
  <generator type="dynetml">
    <!-- Load from File -->
    <param name="filesystem_path" value="construct::stringvar::ora_input_fname" />
    <param name="network_name" value="agent x knowledge" />
    <param name="transpose" value="false" /> <!-- transpose after reading? optional
param, default = false -->
```

```
<rows first="0" last="nodeclass::agent::count_minus_one" />
<cols first="0" last="nodeclass::knowledge::count_minus_one" />
</generator>
<generator type="randomnormal">
  <!-- insert level 1 plan data randomly into all Key IT systems & JPG with low
density random normal -->
  <rows groups="it_agent_key_group.jpg_joint_planning_group"
group_membership_network="agent group membership network" />
  <cols groups="plan_k_level1" group_membership_network="knowledge group
membership network" />
  <param name="mean" value="0.1"/>
  <param name="variance" value="0.02"/>
</generator>
<generator type="randomnormal">
  <!-- insert level 2 plan data into level 2 Key IT systems with high density erdos
renyi, as orders come through electronically -->
  <!-- 28 Mar 15, erdos renyi generate was causing a seg fault when row count != col
count so moved back to random normal generator-->
  <rows groups="it_agent_key_level2_group.jpg_level2"
group_membership_network="agent group membership network" />
  <cols groups="plan_k_level2" group_membership_network="knowledge group
membership network" />
  <param name="mean" value="0.1"/>
  <param name="variance" value="0.02"/>
</generator>
<generator type="randomnormal">
  <!-- insert level 1 plan data into JPG with lower density erdos renyi, as orders come
through electronically -->
  <!-- 28 Mar 15, erdos renyi generate was causing a seg fault when row count != col
count so moved back to random normal generator-->
  <rows groups="jpg_joint_planning_group" group_membership_network="agent
group membership network" />
  <cols groups="plan_k_level2" group_membership_network="knowledge group
membership network" />
  <param name="mean" value="0.2"/>
  <param name="variance" value="0.08"/>
</generator>
<generator type="constant">
  <!-- link integrity agent with bad plan data when i_attack_prob > 0. Keeping links
out of the ORA file reduces the chance
of knowledge leakage through TM perceptions of the integrity agent(s) -->
  <rows groups="integrity_agent_level1_group" group_membership_network="agent
group membership network" />
  <cols groups="bad_plan_k_level1" group_membership_network="knowledge
group membership network" />
  <param name="constant_value" value="1" />
```


Appendix 6 Construct input deck for operational and strategic simulation

```
</generator>
</network>
<network src_nodeclass_type="agent" target_nodeclass_type="knowledge"
id="knowledge priority network" link_type="int" network_type="dense">
  <!-- for each agent, weight the ego places on the specific knowledge bits when picking
knowledge to send to the chosen interaction partner -->
  <!-- Default values-->
  <generator type="constant">
    <rows first="0" last="nodeclass::agent::count_minus_one" />
    <cols first="0" last="nodeclass::knowledge::count_minus_one" />
    <param name="constant_value" value="construct::intvar::knowledge_priority" />
  </generator>
  <generator type="constant">
    <rows groups="jpg_joint_planning_group.jpg_briefing"
group_membership_network="agent group membership network" />
    <cols groups="plan_k,bad_plan_k" group_membership_network="knowledge
group membership network" />
    <param name="constant_value" value="construct::intvar::knowledge_plan_priority"
/>
  </generator>
  <generator type="constant">
    <!-- Zero out integrity agent priority network -->
    <rows groups="integrity_agent_group" group_membership_network="agent group
membership network" />
    <cols first="0" last="nodeclass::knowledge::count_minus_one" />
    <param name="constant_value" value="construct::intvar::knowledge_plan_priority"
/>
  </generator>
  <generator type="constant">
    <!-- now only give priority to bad knowledge for the integrity agent -->
    <rows groups="integrity_agent_group" group_membership_network="agent group
membership network" />
    <cols groups="bad_plan_k" group_membership_network="knowledge group
membership network" />
    <param name="constant_value" value="construct::intvar::knowledge_plan_priority"
/>
  </generator>
</network>
<network src_nodeclass_type="agent" target_nodeclass_type="timeperiod"
id="knowledge similarity weight network" link_type="float" network_type="dense">
  <!-- weight each ego gives to knowledge bits it shares with alters when deciding with
whom to interact -->
  <generator type="randomnormal">
    <!--default values -->
    <rows first="0" last="nodeclass::agent::count_minus_one" />
    <cols first="0" last="nodeclass::timeperiod::count_minus_one" />
```

```
    <param name="mean" value="0.6" />
    <param name="variance" value="0.06" />
  </generator>
  <generator type="randomnormal">
    <rows groups="jpg_joint_planning_group" group_membership_network="agent
group membership network" />
    <cols values="construct::stringvar::planning_timeperiod_list" />
    <param name="mean" value="0.7" />
    <param name="variance" value="0.07" />
  </generator>
  <generator type="randomuniform">
    <rows groups="jpg_briefing" group_membership_network="agent group
membership network" />
    <cols values="construct::stringvar::plan_briefing_time_list" />
    <param name="min" value="0.2" />
    <param name="max" value="0.5" />
  </generator>
</network>
<network src_nodeclass_type="agent" target_nodeclass_type="knowledge" id="learnable
knowledge network" link_type="bool" network_type="dense">
  <generator type="constant">
    <!-- all knowledge is learnable -->
    <rows first="0" last="nodeclass::agent::count_minus_one" />
    <cols first="0" last="nodeclass::knowledge::count_minus_one" />
    <param name="constant_value" value="1" />
  </generator>
</network>
<network src_nodeclass_type="CommunicationMedium"
target_nodeclass_type="knowledge" id="medium knowledgegroup network"
link_type="bool" network_type="dense">
  <!-- CommunicationMedium x knowledge group assignment...iow, which groups do
the mediums support? -->
  <!-- @TODO Fix this so knowledge is not controlled in such an absolutist manner
  <!-- it is more likely that all knowledge groups can go over all comms mediums/media
-->
  <!-- In the mean time, load from File the network manually constructed in the ORA
file-->
  <generator type="dynetml">
    <param name="filesystem_path" value="construct::stringvar::ora_input_fname" />
    <param name="network_name" value="knowledge x comms_media" />
    <param name="transpose" value="true" /> <!-- transpose after reading? optional
param, default = false -->
    <rows first="0" last="nodeclass::CommunicationMedium::count_minus_one" />
    <cols first="0" last="nodeclass::knowledgegroup::count_minus_one" />
  </generator>
</network>
```

Appendix 6 Construct input deck for operational and strategic simulation

```
<network src_nodeclass_type="agent" target_nodeclass_type="agent" id="physical
proximity network" link_type="float" network_type="dense">
  <!-- proximity of agents to each other. Zero(0) ==> maximally distant with each other
with one(1)==>maximally close) -->
  <generator type="dynetml">
    <param name="filesystem_path" value="construct::stringvar::ora_input_fname" />
    <param name="network_name" value="physical proximity" />
    <param name="transpose" value="false" />
    <rows first="0" last="nodeclass::agent::count_minus_one" />
    <cols first="0" last="nodeclass::agent::count_minus_one" />
  </generator>
</network>
<network src_nodeclass_type="agent" target_nodeclass_type="timeperiod" id="physical
proximity weight network" link_type="float" network_type="dense">
  <!--default values -->
  <generator type="randomnormal">
    <rows first="0" last="nodeclass::agent::count_minus_one" />
    <cols first="0" last="nodeclass::timeperiod::count_minus_one" />
    <param name="mean" value="0.6" />
    <param name="variance" value="0.06" />
  </generator>
  <generator type="constant">
    <!-- IT agents don't care about physical proximity, including integrity agents (as IT)
-->
    <rows groups="it_agent_group" group_membership_network="agent group
membership network" />
    <cols first="0" last="nodeclass::timeperiod::count_minus_one" />
    <param name="constant_value" value="1.0" />
  </generator>
  <generator type="randomnormal">
    <!-- during briefings, agents are nudged to talk with other close by agents -->
    <rows groups="jpg_briefing" group_membership_network="agent group
membership network" />
    <cols values="construct::stringvar::plan_briefing_time_list" />
    <param name="mean" value="0.9" />
    <param name="variance" value="0.09" />
  </generator>
  <generator type="randomnormal">
    <!-- during planning time, planning agents are nudged to talk with other close by
agents -->
    <rows groups="jpg_joint_planning_group" group_membership_network="agent
group membership network" />
    <cols values="construct::stringvar::planning_timeperiod_list" />
    <param name="mean" value="0.9" />
    <param name="variance" value="0.09" />
  </generator>
```

```
</network>
<network src_nodeclass_type="agent" target_nodeclass_type="dummy_nodeclass"
id="public message propensity network" link_type="float" network_type="dense">
  <!-- Not used in this model, so all zeros -->
  <generator type="constant">
    <rows first="0" last="nodeclass::agent::count_minus_one" />
    <cols first="0" last="nodeclass::dummy_nodeclass::count_minus_one" />
    <param name="constant_value" value="0.0" />
  </generator>
</network>
<network src_nodeclass_type="agent" target_nodeclass_type="agent"
id="sociodemographic proximity network" link_type="float" network_type="dense">
  <!-- proximity of agents to each other. Zero(0) ==> maximally distant with each other
with one(1)==>maximally close) -->
  <!-- random values for human agent in the absence of empirical data, it agents don't
care so they stay with default of 0 -->
  <generator type="randomnormal">
    <rows groups="human_agent_group" group_membership_network="agent group
membership network" />
    <cols groups="human_agent_group" group_membership_network="agent group
membership network" />
    <param name="mean" value="0.2" />
    <param name="variance" value="0.02" />
  </generator>
</network>
<network src_nodeclass_type="agent" target_nodeclass_type="timeperiod"
id="sociodemographic proximity weight network" link_type="float" network_type="dense">
  <generator type="constant">
    <!-- default value = 0.01 for all agents-->
    <rows first="0" last="nodeclass::agent::count_minus_one" />
    <cols first="0" last="nodeclass::timeperiod::count_minus_one" />
    <param name="constant_value" value="0.01" />
  </generator>
  <generator type="randomnormal">
    <!-- random values for human agent in the absence of empirical data -->
    <rows groups="human_agent_group" group_membership_network="agent group
membership network" />
    <cols first="0" last="nodeclass::timeperiod::count_minus_one" />
    <param name="mean" value="0.2" />
    <param name="variance" value="0.02" />
  </generator>
</network>
<network src_nodeclass_type="agent" target_nodeclass_type="agent" id="social
proximity network" link_type="float" network_type="dense">
  <!-- proximity of agents to each other. Zero(0) ==> maximally distant with each other
with one(1)==>maximally close) -->
```

Appendix 6 Construct input deck for operational and strategic simulation

```

<generator type="constant">
  <!-- default value = 0.01 for all agents-->
  <rows first="0" last="nodeclass::agent::count_minus_one" />
  <cols first="0" last="nodeclass::timeperiod::count_minus_one" />
  <param name="constant_value" value="0.01" />
</generator>
<!-- random values for human agent in the absence of empirical data -->
<generator type="randomnormal">
  <rows groups="human_agent_group" group_membership_network="agent group
membership network" />
  <cols groups="human_agent_group" group_membership_network="agent group
membership network" />
  <param name="mean" value="0.6" />
  <param name="variance" value="0.06" />
</generator>
</network>
<network src_nodeclass_type="agent" target_nodeclass_type="timeperiod" id="social
proximity weight network" link_type="float" network_type="dense">
  <!-- when picking an interaction partner, weight ego uses to develop probability of
interaction -->
  <generator type="constant">
    <!-- default value = 0 for all agents-->
    <rows first="0" last="nodeclass::agent::count_minus_one" />
    <cols first="0" last="nodeclass::timeperiod::count_minus_one" />
    <param name="constant_value" value="0.01" />
  </generator>
  <generator type="randomnormal">
    <!-- random values for human agent in the absence of empirical data -->
    <rows groups="human_agent_group" group_membership_network="agent group
membership network" />
    <cols first="0" last="nodeclass::timeperiod::count_minus_one" />
    <param name="mean" value="0.4" />
    <param name="variance" value="0.04" />
  </generator>
</network>
<network src_nodeclass_type="agent" target_nodeclass_type="knowledge"
id="transmission knowledge weight network" link_type="float" network_type="dense">
  <!-- when picking knowledge to transmit to alters, weight assigned to each knowledge
bit for inclusion in messages -->
  <generator type="constant">
    <rows first="0" last="nodeclass::agent::count_minus_one" />
    <cols first="0" last="nodeclass::knowledge::count_minus_one" />
    <param name="constant_value" value="construct::intvar::knowledge_priority" />
  </generator>
  <generator type="constant">
    <rows first="0" last="nodeclass::agent::count_minus_one" />

```

```

    <cols groups="plan_k,bad_plan_k" group_membership_network="knowledge
group membership network" />
    <param name="constant_value" value="construct::intvar::knowledge_plan_priority"
/>
  </generator>
  <!-- integrity agents like to transmit nothing but bad plan knowledge -->
  <generator type="constant">
    <rows groups="integrity_agent_group" group_membership_network="agent group
membership network" />
    <cols groups="no_bad_k" group_membership_network="knowledge group
membership network" />
    <param name="constant_value" value="0" />
  </generator>
</network>
</networks>

<!-- ***** _
>
<!-- INITIAL TRANSACTIVE MEMORY VALUES -->
<!-- these are agent perceptions of others -->
<!-- ***** _
>
<transactivememory>
  <network id="knowledge transactive memory network" ego_nodeclass_type="agent"
src_nodeclass_type="agent" target_nodeclass_type="knowledge" link_type="bool"
network_type="TMBool" associated_network="knowledge network">
    <!-- default random values created from random_value < false positive and negative
rates and omniscient knowledge value -->
    <!-- shifted away from perception based to group based for use with multi-level TM --
>
    <generator type="group_based">
      <!-- ignore transactive memory about and for the integrity and confidentiality
agents-->
      <ego first="0" last="nodeclass::agent::count_minus_one - 2"/>
      <alter first="0" last="nodeclass::agent::count_minus_one - 2"/>
      <transactive first="0" last="construct::intvar::knowledge_general_count +
construct::intvar::knowledge_plan_count - 1"/>
      <param name="name" value="initial_KTM_group_to_group_for_no_bad_k" />

      <param name="group_flip_to_positive_rate"
value="construct::floatvar::group_flip_to_positive_rate"/>
      <param name="group_flip_to_negative_rate"
value="construct::floatvar::group_flip_to_negative_rate"/>
      <param name="agent_flip_to_positive_rate"
value="construct::floatvar::agent_flip_to_positive_rate"/>

```

Appendix 6 Construct input deck for operational and strategic simulation

```
<param name="agent_flip_to_negative_rate"
value="construct::floatvar::agent_flip_to_negative_rate"/>
<param name="verbose" value="false"/>
<param name="verbosity_frequency" value="50"/> <!-- ** display every nth agent
** -->
</generator>
<generator type="group_based">
<!-- ignore transactive memory about and for the integrity and confidentiality
agents-->
<ego values="construct::agentgroupvar::non_integrity_agent_group"/>
<alter values="construct::agentgroupvar::integrity_agent_group"/>
<transactive first="construct::intvar::knowledge_general_count +
construct::intvar::knowledge_plan_count" last="nodeclass::knowledge::count_minus_one"/>
<param name="name" value="initial_KTM_group_to_group_for_bad_k_only" />

<param name="group_flip_to_positive_rate" value="0.0"/>
<param name="group_flip_to_negative_rate" value="1.0"/>
<param name="agent_flip_to_positive_rate" value="0.0"/>
<param name="agent_flip_to_negative_rate" value="1.0"/>
<param name="verbose" value="true"/>
<param name="verbosity_frequency" value="1"/> <!-- ** display every nth agent **
-->
</generator>
</network>
<network id="binarytask transactive memory network" ego_nodeclass_type="agent"
src_nodeclass_type="agent" target_nodeclass_type="binarytask" link_type="bool"
network_type="TMBool" associated_network="binarytask assignment network">
<generator type="group_based">
<ego first="0" last="nodeclass::agent::count - 3"/>
<alter first="0" last="nodeclass::agent::count - 3"/>
<transactive first="0" last="nodeclass::knowledge::count_minus_one"/>
<param name="name" value="initial_BinaryTaskTM_group_to_group" />

<param name="group_flip_to_positive_rate"
value="construct::floatvar::group_flip_to_positive_rate"/>
<param name="group_flip_to_negative_rate"
value="construct::floatvar::group_flip_to_negative_rate"/>
<param name="agent_flip_to_positive_rate"
value="construct::floatvar::agent_flip_to_positive_rate"/>
<param name="agent_flip_to_negative_rate"
value="construct::floatvar::agent_flip_to_negative_rate"/>
<param name="verbose" value="true"/>
</generator>
</network>
</transactivememory>
<!-- ***** -->
```

```
<!-- OPERATIONS FOR SIMULATION OUTPUT -->
<!-- these are the values that are printed and/or saved -->
<!-- ***** -->
<operations>
<operation name="Nodeset_dump"><!-- Dump agent nodeset for ease of agent_n to
agent_name conversions -->
<parameters>
<param name="nodeset_name" value="agent"/>
<param name="output_filename" value="agent_nodeset.csv"/>
<param name="print_col_names" value="true" /> <!-- default=false-->
<param name="print_row_numbers" value="true" /> <!-- default=false-->
<param name="output_format" value="csv"/>
<param name="run" value="all"/>
<param name="time" value="0"/>
<param name="verbose" value="false"/> <!-- optional, default=false-->
</parameters>
</operation>
<operation name="Nodeset_dump"><!-- Dump agent nodeset for ease of agent_n to
agent_name conversions -->
<parameters>
<param name="nodeset_name" value="agentgroup"/>
<param name="output_filename" value="agentgroup_nodeset.csv"/>
<param name="print_col_names" value="true" /> <!-- default=false-->
<param name="print_row_numbers" value="true" /> <!-- default=false-->
<param name="output_format" value="csv"/>
<param name="run" value="all"/>
<param name="time" value="0"/>
<param name="verbose" value="false"/> <!-- optional, default=false-->
</parameters>
</operation>
<operation name="AvgProbInteractOverRuns"><!-- print average of interaction
probability per agent-->
<parameters>
<param name="output_filename" value="avgProbabilityOfInteraction.csv"/>
<param name="output_format" value="csv"/>
<param name="time" value="all"/>
<param name="output_format" value="csv" />
<param name="print_row_numbers" value="true" />
<param name="print_col_names" value="true" />
<param name="print_run_and_timeperiod" value="true" />
</parameters>
</operation><!-- these operations help test that Construct read the graphs of the dynetml
file correctly -->
<operation name="ReadGraphByName"><!-- Printing the agent x agent access network
before and during the attack helps modeler confirm/deny the as-evolved networks == as-
designed networks -->
```

Appendix 6 Construct input deck for operational and strategic simulation

```
<parameters>
  <param name="graph_name" value="access network"/>
  <param name="output_filename"
value="agent_access_network_attack_times.csv"/>
  <param name="output_format" value="csv"/>
  <param name="run" value="all"/>
  <param name="time" value="attacktime_output_list"/>
  <param name="operation_name" value="dump_access_network" />
  <param name="operation_subname" value="all_time_periods" />
  <param name="print_row_numbers" value="true" />
  <param name="print_row_names" value="true" />
  <param name="print_col_numbers" value="true" />
  <param name="no_empty_lines " value="true" />
  <param name="print_run_and_timeperiod" value="true" />
</parameters>
</operation>
<operation name="ReadGraphByName"> <!-- Printing the agent x communication
medium access network before & during attack helps modeler confirm/deny the as-evolved
networks == as-designed networks -->
  <parameters>
    <param name="graph_name" value="communication medium access network"/>
    <param name="output_filename"
value="agent_comms_media_access_network_attack_times.csv"/>
    <param name="output_format" value="csv"/>
    <param name="run" value="all"/>
    <param name="time" value="all"/>
    <!--
--> <param name="time" value="construct::stringvar::attacktime_output_list"/>
    <param name="operation_name" value="dump_access_network" />
    <param name="operation_subname" value="all_time_periods" />
    <param name="print_row_numbers" value="true" />
    <param name="print_row_names" value="true" />
    <param name="print_col_numbers" value="true" />
    <param name="print_col_names" value="true" />
    <param name="no_empty_lines " value="true" />
    <param name="print_run_and_timeperiod" value="true" />
  </parameters>
</operation>
<operation name="ReadGraphKTM"> <!-- print KTM 3D for first 11 time periods -->
  <parameters>
    <param name="output_filename" value="KTM_first_ten.csv"/>
    <param name="output_format" value="csv"/>
    <param name="run" value="0"/>
    <param name="print_run_and_timeperiod" value="true" />
    <param name="print_ego_numbers" value="true" /> <!-- default false-->
    <param name="print_ego_names" value="true" /> <!-- default false-->
    <param name="print_alter_numbers" value="true" /> <!-- default false-->
```

```
    <param name="print_alter_names" value="true" /> <!-- default false-->
    <param name="print_k_numbers" value="true" /> <!-- default false-->
    <param name="print_k_names" value="true" /> <!-- default false-->
    <param name="no_empty_lines" value="true" /> <!-- default true-->
    <param name="time" value="0..10"/>
  </parameters>
</operation>
<operation name="ReadGraphByName"> <!-- Printing the agent x active timeperiod
network before and during the attack helps modeler confirm/deny the as-evolved networks ==
as-designed networks -->
  <parameters>
    <param name="graph_name" value="agent active timeperiod network"/>
    <param name="output_filename"
value="agent_active_timeperiod_network_attack_times.csv"/>
    <param name="output_format" value="csv"/>
    <param name="run" value="all"/>
    <param name="time" value="attacktime_output_list"/>
    <param name="operation_name" value="dump_agent_active_timeperiod_network"
/>
    <param name="operation_subname" value="all_time_periods" />
    <param name="print_row_numbers" value="true" />
    <param name="print_row_names" value="true" />
    <param name="print_col_names" value="true" />
    <param name="no_empty_lines " value="true" />
    <param name="print_run_and_timeperiod" value="true" />
  </parameters>
</operation>
<operation name="ReadGraphByName"> <!-- Printing the agent x dummy network that
specifies the agent type at time 0 helps modeler confirm/deny the as-evolved networks == as-
designed networks -->
  <parameters>
    <param name="graph_name" value="agent active timeperiod network"/>
    <param name="output_filename"
value="agent_active_timeperiod_network_0.csv"/>
    <param name="output_format" value="csv"/>
    <param name="run" value="all"/>
    <param name="time" value="0"/>
    <param name="operation_name" value="dump_agent_active_timeperiod_network"
/>
    <param name="operation_subname" value="time_zero" />
    <param name="print_row_numbers" value="true" />
    <param name="print_row_names" value="true" />
    <param name="print_col_names" value="true" />
    <param name="no_empty_lines " value="true" />
    <param name="print_run_and_timeperiod" value="true" />
  </parameters>
```

Appendix 6 Construct input deck for operational and strategic simulation

```
</operation>
<operation name="ReadGraphByName"> <!-- Printing the agent x knowledge network
supports exogenous to Construct analysis of knowledge based
metrics, every ten percent of the run, during attack times (+/- 1) and during brief times
-->
  <parameters>
    <param name="graph_name" value="knowledge network"/>
    <param name="output_filename" value="knowledge_over_time.csv"/>
    <param name="output_format" value="csv"/>
    <param name="run" value="all"/>
    <!--<param name="time"
value="output_by_percentiles,attacktime_output_list,plan_briefing_time_list"/>-->
    <param name="time" value="all"/>
    <param name="operation_name" value="dump_agent_knowledge_network" />
    <!--<param name="operation_subname"
value="ten_percent_attacktime_output_list_plan_briefing_time_list" />-->
    <param name="operation_subname" value="all_time_periods" />
    <param name="print_row_numbers" value="true" />
    <param name="print_row_names" value="true" />
    <param name="print_col_numbers" value="true" />
    <param name="print_col_names" value="true" />
    <param name="no_empty_lines" value="true" />
    <param name="print_run_and_timeperiod" value="true" />
  </parameters>
</operation>
<operation name="ReadGraphByName"> <!-- Printing interaction network at all times --
>
  <parameters>
    <param name="graph_name" value="interaction network"/>
    <param name="output_filename" value="interaction_all.csv"/>
    <param name="output_format" value="csv"/>
    <param name="run" value="all"/>
    <param name="operation_name" value="dump_interaction_network_network" />
    <param name="operation_subname" value="all_time_periods" />
    <param name="print_row_numbers" value="true" />
    <param name="print_row_names" value="true" />
    <param name="print_col_numbers" value="true" />
    <param name="print_col_names" value="true" />
    <param name="no_empty_lines" value="true" />
    <param name="print_run_and_timeperiod" value="true" />
  </parameters>
</operation>
<operation name="ReadKnowledgeLearningHistory"> <!-- Print the knowledge
learning history for first 11 time periods -->
  <parameters>
    <param name="output_filename" value="knowledge_history_all.csv"/>
```

```
    <param name="output_format" value="csv"/>
    <param name="run" value="all"/>
    <param name="time" value="0,1,2,3,4,5,6,7,8,9,10" />
    <param name="operation_name" value="dump_knowledge_history" />
    <param name="operation_subname" value="first_ten_time_periods" />
    <param name="print_row_numbers" value="true" />
    <param name="print_col_numbers" value="true" />
    <param name="print_row_names" value="true" />
    <param name="print_col_names" value="true" />
    <param name="no_empty_lines" value="true" />
    <param name="print_run_and_timeperiod" value="true" />
  </parameters>
</operation>
<operation name="ReadKnowledgeDiffusionByAgentGroup"> <!--
diffusion_by_group_all -->
  <parameters>
    <param name="graph_name" value="knowledge network"/>
    <param name="output_filename" value="diffusion_by_group_all.csv"/>
    <param name="output_format" value="csv"/>
    <param name="run" value="all"/>
    <param name="time" value="output_by_percentiles" />
    <param name="operation_name" value="dump_knowledge_diffusion_network" />
    <param name="operation_subname" value="every_ten_percent" />
    <param name="print_run_and_timeperiod" value="true" />
    <param name="print_row_numbers" value="true" />
    <param name="print_col_numbers" value="true" />
    <param name="print_row_names" value="true" />
    <param name="print_col_names" value="true" />
    <!--
    <param name="verbose" value="true" />
    -->
  </parameters>
</operation>
<operation name="KnowledgeDiffusionByIndexRange"> <!-- Print the bad plan
knowledge diffusion-->
  <parameters>
    <param name="graph_name" value="knowledge network"/>
    <param name="output_filename" value="bad_plan_k_all.csv"/>
    <param name="output_format" value="csv"/>
    <param name="run" value="all"/>
    <param name="time" value="output_by_percentiles" />
    <param name="operation_name"
value="dump_knowledge_diffusion_bad_plan_only" />
    <param name="operation_subname" value="every_ten_percent" />
    <param name="print_run_and_timeperiod" value="true" />
    <param name="print_row_numbers" value="true" />
    <param name="print_col_numbers" value="true" />
    <param name="print_row_names" value="true" />
```

Appendix 6 Construct input deck for operational and strategic simulation

```
<!-- <param name="print_col_names" value="true" />
--> <param name="verbose" value="true" />
--> <param name="index_list" value="construct::knowledgegroupvar::bad_plan_k" />
</parameters>
</operation>
<operation name="KnowledgeDiffusionByIndexRange"> <!-- Print the non-bad
knowledge (plan and non-plan)-->
<parameters>
  <param name="graph_name" value="knowledge network"/>
  <param name="output_filename" value="non_bad_diffusion_all.csv"/>
  <param name="output_format" value="csv"/>
  <param name="run" value="all"/>
  <param name="time" value="all" />
  <param name="operation_name" value="dump_non_bad_diffusion_all" />
  <param name="operation_subname" value="all_time_periods" />
  <param name="print_run_and_timeperiod" value="true" />
  <param name="print_row_numbers" value="true" />
  <param name="print_col_numbers" value="true" />
  <param name="print_row_names" value="true" />
  <param name="print_col_names" value="true" />
<!-- <param name="verbose" value="true" />
--> <param name="index_list" value="construct::knowledgegroupvar::no_bad_k" />
</parameters>
</operation>
<operation name="ReadKnowledgeDiffusion"> <!-- print knowledge diffusion stats, all
times -->
<parameters>
  <param name="graph_name" value="knowledge network"/>
  <param name="output_filename" value="diffusion_all.csv"/>
  <param name="output_format" value="csv"/>
  <param name="run" value="all"/>
  <param name="time" value="all" />
  <param name="operation_name" value="dump_diffusion_all" />
  <param name="operation_subname" value="all_time_periods" />
  <param name="print_run_and_timeperiod" value="true" />
  <param name="print_row_numbers" value="true" />
  <param name="print_col_numbers" value="true" />
  <param name="print_row_names" value="true" />
  <param name="print_col_names" value="true" />
</parameters>
</operation>
<operation name="ReadAgentsWhoDoNotInteractWithAnyone">
<parameters>
  <param name="output_filename"
value="AgentsWhoDoNotInteractWithAnyone.csv"/>
  <param name="output_format" value="csv"/>
```

```
<param name="output_to_stdout" value="true"/>
<param name="print_row_names" value="true" />
<param name="print_col_names" value="true" />
<param name="print_row_numbers" value="true" />
<param name="print_col_numbers" value="true" />
<param name="print_run_and_timeperiod" value="true" />
<param name="run" value="all"/>
<param name="time" value="all"/>
<param name="operation_name" value="dump_agents_who_dont_interact" />
<param name="operation_subname" value="all_time_periods" />
</parameters>
</operation>

<operation name="ReadAgentCoreTies">
<parameters>
  <param name="output_filename" value="agent_core_ties_first_eleven.csv"/>
  <param name="output_format" value="csv"/>
  <param name="time" value="0..10"/>
  <param name="print_run_and_timeperiod" value="true" />
  <param name="print_row_names" value="true" />
  <param name="print_col_names" value="true" />
  <param name="print_row_numbers" value="true" />
  <param name="print_col_numbers" value="true" />
  <param name="activation_score_as_edge_weight" value="true"/>
</parameters>
</operation>

<operation name="ActivateAltersForAgents"><!-- Used to make agents aware of a
new/old set of alters with some probability at the
specified time (post attack + 1) new awareness will stick. Use Case: A message to all
agents of who the 'chain of command' is
ActivateAltersForAgents validated output == reasonable 28 Jan 15 -->
<parameters>
  <param name="output_filename" value="activateAlters_0.csv"/>
  <param name="output_format" value="csv"/>
  <param name="time" value="0,1"/>
  <param name="activation_network_filename"
value="starting_active_Alters_edgeList.csv"/>
  <param name="symmetric_flag" value="false"/>
  <param name="load_style" value="sparse_to_dense_convert" />
  <param name="skip_first_row" value="true" />
  <param name="probability_of_activation" value=".9"/>
</parameters>
</operation>

<!-- <operation name="ActivateAltersForAgents"> <!-- ActivateAltersForAgents validated
output == reasonable 28 Jan 15 -->
<!--
```

Appendix 6 Construct input deck for operational and strategic simulation

```

<parameters>
  <param name="output_filename" value="activateAlters_343.csv"/>
  <param name="output_format" value="csv"/>
  <param name="time" value="construct::intvar::attack_end_time+1"/>
  <param name="activation_network_filename"
value="activateAlters_edgeList.csv"/>
  <param name="symmetric_flag" value="false"/>
  <param name="load_style" value="sparse_to_dense_convert" />
  <param name="skip_first_row" value="true" />
  <param name="probability_of_activation" value=".5"/>
</parameters>
</operation>
-->
  <!-- Allows experimenter to force a recalculation by ego's of their transactive memory of
groups in the sim
  Use Case: Can be used if some substantial change has occurred and simulator needs to tell
all agents
  to reassess their understanding of the world -->
<!-- <operation name="ForceLossyIntersection">
  <parameters>
    <param name="time" value="all"/>
  </parameters>
</operation>
-->
  <!-- Prints per agent perception of groups' knowledge -->
<!-- <operation name="ReadAgentBeliefOfGroupKnowledgeMatrix"> <!-- -->
<!-- <parameters>
  <param name="output_filename" value="AvgAgentBeliefOfGroupKnowledge.csv"/>
  <param name="output_format" value="csv"/>
  <param name="time" value="all"/>
</parameters>
</operation>
-->
<!-- <operation name="CommunicationMediumsSent"> <!-- -->
<!-- <parameters>
  <param name="output_filename" value="Communications_Mediums_Sent_all.csv"
/>
  <param name="output_format" value="csv" />
  <param name="print_row_names" value="true" />
  <param name="print_col_names" value="true" />
  <param name="print_run_and_timeperiod" value="true" />
  <param name="time" value="all" />
</parameters>
</operation>
<!-- <operation name="CommunicationMediumsReceived"> <!-- -->
<!-- <parameters>

```

```

  <param name="output_filename"
value="Communications_Mediums_Received_all.csv" />
  <param name="output_format" value="csv" />
  <param name="print_row_names" value="true" />
  <param name="print_col_names" value="true" />
  <param name="print_run_and_timeperiod" value="true" />
  <param name="time" value="all" />
</parameters>
</operation>
-->

  <!-- availability attacks not specifically targeting key IT systems are targeting the
communications mechanisms -->

  <operation name="ReadGeneralDecisionOutput"><!-- Use ReadGeneralDecisionOutput
to turn agent x communicationMediums on/off
  as a function of being during the attack time windows, and based on a probabilistic
random draw being less than the
modeler specified threshold -->
  <parameters>
    <param name="verbose" value="true" />
    <param name="run" value="all"/>
    <param name="time" value="attack_time_list_plus_one"/>
    <param name="output_filename" value="turn_comms_media_off_and_on.csv"/>
    <param name="output_format" value="csv"/>
    <param name="header_row" value="true"/>
    <param name="applicable_agents"
value="construct::agentgroupvar::non_integrity_agent_group"/>
    <param name="decision_names"
value="a_attack_web_off,a_attack_phone_off,a_attack_email_off,turn_agents_comms_on" />
    <param name="a_attack_email_off" value="1" />
    <param name="a_attack_web_off" value="
if ((construct::boolvar::attack_enabled) && (timeperiod >
construct::intvar::warm_up_period)
  && (randomUniform(0.0,1.0) < construct::floatvar::a_attack_web_prob)
  && (timeperiod ≤ construct::intvar::attack_end_time))
{ /* setFooNetwork returns the value being set, multiple sets can occur by chaining
them with a boolean AND operator to cause all to execute */
  setCommunicationMediumAccessNetwork[agent,construct::intvar::web_lv1,0.0]
&
  setCommunicationMediumAccessNetwork[agent,construct::intvar::web_lv2,0.0]
} else {
  1 /* non-harm else statement */
} " with="agent,verbose,timeperiod" />

```


Appendix 6 Construct input deck for operational and strategic simulation

```
<param name="a_attack_phone_off" value="
  if ((construct::boolvar::attack_enabled) && (timeperiod >
construct::intvar::warm_up_period)
    && (randomUniform(0.0,1.0) < construct::floatvar::a_attack_phone_prob)
    && (timeperiod ≤ construct::intvar::attack_end_time)){

setCommunicationMediumAccessNetwork[agent,construct::intvar::phone_lv11,0.0] &

setCommunicationMediumAccessNetwork[agent,construct::intvar::phone_lv12,0.0]
  } else {
    1 /* non-harm else statement */
  }" with="agent,verbose,timeperiod" />
<param name="a_attack_email_off" value="
  if (construct::boolvar::attack_enabled && (timeperiod >
construct::intvar::warm_up_period)
    && (randomUniform(0.0,1.0) < construct::floatvar::a_attack_email_prob)
    && (timeperiod ≤ construct::intvar::attack_end_time)){

setCommunicationMediumAccessNetwork[agent,construct::intvar::email_lv11,0.0] &

setCommunicationMediumAccessNetwork[agent,construct::intvar::email_lv12,0.0]
  } else {
    1 /* non-harm else statement */
  }" with="agent,verbose,timeperiod" />
<!-- Use ReadGeneralDecisionOutput to turn agent x communicationMediums on after
attack as a function
of the agent being level1 or level2, or level 2, attacks were enabled, and attacks have
ended -->
<param name="turn_agents_comms_on" value="
  if (construct::boolvar::attack_enabled && (timeperiod >=
(construct::intvar::attack_end_time+1))) {
    foreach $al2$ (construct::agentgroupvar::human_agent_level2_group){

setCommunicationMediumAccessNetwork[$al2$,construct::intvar::web_lv11,1.0] &

setCommunicationMediumAccessNetwork[$al2$,construct::intvar::web_lv12,1.0] &
```

```
setCommunicationMediumAccessNetwork[$al2$,construct::intvar::phone_lv11,1.0] &

setCommunicationMediumAccessNetwork[$al2$,construct::intvar::phone_lv12,1.0] &

setCommunicationMediumAccessNetwork[$al2$,construct::intvar::email_lv12,1.0] &

setCommunicationMediumAccessNetwork[$al2$,construct::intvar::email_lv11,1.0]
  } &
  foreach $al1$ (construct::agentgroupvar::human_agent_level1_group){

setCommunicationMediumAccessNetwork[$al1$,construct::intvar::web_lv11,1.0] &

setCommunicationMediumAccessNetwork[$al1$,construct::intvar::phone_lv11,1.0] &

setCommunicationMediumAccessNetwork[$al1$,construct::intvar::email_lv12,1.0] &
  } &
  foreach $al2$ (construct::agentgroupvar::it_agent_level2_group){

setCommunicationMediumAccessNetwork[$al2$,construct::intvar::web_lv12,1.0]
  } &
  foreach $al1$ (construct::agentgroupvar::it_agent_level1_group){

setCommunicationMediumAccessNetwork[$al1$,construct::intvar::web_lv11,1.0]
  }
  } else {
    1 /* non-harm else statement */
  }" with="verbose,timeperiod" />
</parameters>
</operation>
</operations>
</construct>
</construct>
```

Appendix 7 Additional Model Analysis, Tables, and Figures

Descriptive Statistics of Operational Model, Attacks, and Mitigations

Descriptive Statistics														
attack severity	Mitigation sum		N Statistic	Range Statistic	Minimum Statistic	Maximum Statistic	Mean Statistic	Std. Error	Std. Dev. Statistic	Variance Statistic	Skewness Statistic	Std Error	Kurtosis Statistic	Std. Error
.00	.31	Plan k (total)	4000	3128	743	3871	2669.02	14.301	904.484	818091.880	-.172	.039	-1.119	.077
		Plan k level1	4000	351	39	390	306.71	1.345	85.094	7240.960	-1.302	.039	1.062	.077
		Plan k level2	4000	2781	704	3485	2362.31	13.063	826.184	682580.481	-.081	.039	-1.218	.077
		Valid N (listwise)	4000											
.20	1.51	Plan k (total)	400	1684	744	2427	1813.79	21.472	429.446	184423.504	-.353	.122	-.858	.243
		Plan k level1	400	288	39	327	254.69	3.751	75.020	5628.042	-1.143	.122	.384	.243
		Plan k level2	400	1400	705	2105	1559.10	17.976	359.522	129255.816	-.187	.122	-1.030	.243
		Valid N (listwise)	400											
	1.54	Plan k (total)	400	1684	744	2427	1813.79	21.472	429.446	184423.504	-.353	.122	-.858	.243
		Plan k level1	400	288	39	327	254.69	3.751	75.020	5628.042	-1.143	.122	.384	.243
		Plan k level2	400	1400	705	2105	1559.10	17.976	359.522	129255.816	-.187	.122	-1.030	.243
		Valid N (listwise)	400											
	1.71	Plan k (total)	400	1684	744	2427	1813.79	21.472	429.446	184423.504	-.353	.122	-.858	.243
		Plan k level1	400	288	39	327	254.69	3.751	75.020	5628.042	-1.143	.122	.384	.243
		Plan k level2	400	1400	705	2105	1559.10	17.976	359.522	129255.816	-.187	.122	-1.030	.243
		Valid N (listwise)	400											
	1.74	Plan k (total)	400	1684	744	2427	1813.79	21.472	429.446	184423.504	-.353	.122	-.858	.243
		Plan k level1	400	288	39	327	254.69	3.751	75.020	5628.042	-1.143	.122	.384	.243
		Plan k level2	400	1400	705	2105	1559.10	17.976	359.522	129255.816	-.187	.122	-1.030	.243
		Valid N (listwise)	400											
	3.51	Plan k (total)	400	1684	744	2427	1813.79	21.472	429.446	184423.504	-.353	.122	-.858	.243
		Plan k level1	400	288	39	327	254.69	3.751	75.020	5628.042	-1.143	.122	.384	.243
		Plan k level2	400	1400	705	2105	1559.10	17.976	359.522	129255.816	-.187	.122	-1.030	.243
		Valid N (listwise)	400											
	3.53	Plan k (total)	400	1684	744	2427	1813.79	21.472	429.446	184423.504	-.353	.122	-.858	.243
		Plan k level1	400	288	39	327	254.69	3.751	75.020	5628.042	-1.143	.122	.384	.243
		Plan k level2	400	1400	705	2105	1559.10	17.976	359.522	129255.816	-.187	.122	-1.030	.243
		Valid N (listwise)	400											

Appendix 7 Additional Model Analysis, Tables, and Figures

Descriptive Statistics

attack severity	Mitigation sum	N Statistic	Range Statistic	Minimum Statistic	Maximum Statistic	Mean		Std. Dev. Statistic	Variance Statistic	Skewness		Kurtosis	
						Statistic	Std. Error			Statistic	Std. Error	Statistic	Std. Error
.40	3.71 Plan k (total)	400	1684	744	2427	1813.79	21.472	429.446	184423.504	-.353	.122	-.858	.243
	Plan k level1	400	288	39	327	254.69	3.751	75.020	5628.042	-1.143	.122	.384	.243
	Plan k level2	400	1400	705	2105	1559.10	17.976	359.522	129255.816	-.187	.122	-1.030	.243
	Valid N (listwise)	400											
	3.74 Plan k (total)	400	1684	744	2427	1813.79	21.472	429.446	184423.504	-.353	.122	-.858	.243
	Plan k level1	400	288	39	327	254.69	3.751	75.020	5628.042	-1.143	.122	.384	.243
	Plan k level2	400	1400	705	2105	1559.10	17.976	359.522	129255.816	-.187	.122	-1.030	.243
	Valid N (listwise)	400											
	.31 Plan k (total)	600	1684	744	2427	1785.51	17.863	437.557	191456.523	-.321	.100	-.937	.199
	Plan k level1	600	289	39	328	247.63	3.031	74.247	5512.649	-1.046	.100	.197	.199
	Plan k level2	600	1400	705	2105	1537.87	14.997	367.350	134945.711	-.176	.100	-1.075	.199
	Valid N (listwise)	600											
	.33 Plan k (total)	500	1722	744	2465	1805.97	19.959	446.300	199183.354	-.329	.109	-.961	.218
	Plan k level1	500	289	39	328	248.40	3.312	74.062	5485.251	-1.054	.109	.239	.218
	Plan k level2	500	1433	705	2138	1557.57	16.807	375.809	141232.338	-.195	.109	-1.107	.218
	Valid N (listwise)	500											
	.34 Plan k (total)	600	1684	744	2427	1785.51	17.863	437.557	191456.523	-.321	.100	-.937	.199
	Plan k level1	600	289	39	328	247.63	3.031	74.247	5512.649	-1.046	.100	.197	.199
	Plan k level2	600	1400	705	2105	1537.87	14.997	367.350	134945.711	-.176	.100	-1.075	.199
	Valid N (listwise)	600											
	.36 Plan k (total)	600	1684	744	2427	1785.51	17.863	437.557	191456.523	-.321	.100	-.937	.199
	Plan k level1	600	289	39	328	247.63	3.031	74.247	5512.649	-1.046	.100	.197	.199
	Plan k level2	600	1400	705	2105	1537.87	14.997	367.350	134945.711	-.176	.100	-1.075	.199
	Valid N (listwise)	600											
	.51 Plan k (total)	500	1699	744	2443	1767.44	19.416	434.151	188486.825	-.282	.109	-.948	.218
	Plan k level1	500	291	39	330	252.35	3.347	74.852	5602.846	-1.033	.109	.222	.218
	Plan k level2	500	1414	705	2119	1515.08	16.241	363.151	131878.745	-.125	.109	-1.084	.218
	Valid N (listwise)	500											
	.53 Plan k (total)	400	1699	744	2443	1784.82	22.248	444.959	197988.840	-.268	.122	-1.002	.243
	Plan k level1	400	285	39	324	248.70	3.643	72.856	5308.032	-1.074	.122	.376	.243
	Plan k level2	400	1414	705	2119	1536.12	18.775	375.502	141001.746	-.129	.122	-1.155	.243
	Valid N (listwise)	400											

Appendix 7 Additional Model Analysis, Tables, and Figures

Descriptive Statistics

attack severity	Mitigation sum	N Statistic	Range Statistic	Minimum Statistic	Maximum Statistic	Mean		Std. Dev. Statistic	Variance Statistic	Skewness		Kurtosis	
						Statistic	Std. Error			Statistic	Std. Error	Statistic	Std. Error
.71	Plan k (total)	400	1699	744	2443	1778.58	22.068	441.358	194796.883	-.273	.122	-.979	.243
	Plan k level1	400	291	39	330	250.24	3.683	73.659	5425.595	-1.053	.122	.304	.243
	Plan k level2	400	1414	705	2119	1528.34	18.570	371.396	137935.085	-.126	.122	-1.125	.243
	Valid N (listwise)	400											
.73	Plan k (total)	600	1699	744	2443	1784.66	18.179	445.291	198284.064	-.274	.100	-.990	.199
	Plan k level1	600	291	39	330	249.80	2.984	73.101	5343.730	-1.054	.100	.300	.199
	Plan k level2	600	1414	705	2119	1534.86	15.341	375.779	141209.915	-.133	.100	-1.136	.199
	Valid N (listwise)	600											
1.31	Plan k (total)	200	1670	744	2413	1810.96	31.140	440.381	193935.626	-.365	.172	-.879	.342
	Plan k level1	200	279	39	318	241.51	5.347	75.617	5717.881	-1.015	.172	.021	.342
	Plan k level2	200	1391	705	2095	1569.45	26.003	367.732	135226.642	-.231	.172	-1.009	.342
	Valid N (listwise)	200											
1.33	Plan k (total)	200	1670	744	2413	1810.96	31.140	440.381	193935.626	-.365	.172	-.879	.342
	Plan k level1	200	279	39	318	241.51	5.347	75.617	5717.881	-1.015	.172	.021	.342
	Plan k level2	200	1391	705	2095	1569.45	26.003	367.732	135226.642	-.231	.172	-1.009	.342
	Valid N (listwise)	200											
3.31	Plan k (total)	200	1670	744	2413	1810.96	31.140	440.381	193935.626	-.365	.172	-.879	.342
	Plan k level1	200	279	39	318	241.51	5.347	75.617	5717.881	-1.015	.172	.021	.342
	Plan k level2	200	1391	705	2095	1569.45	26.003	367.732	135226.642	-.231	.172	-1.009	.342
	Valid N (listwise)	200											
3.33	Plan k (total)	200	1670	744	2413	1810.96	31.140	440.381	193935.626	-.365	.172	-.879	.342
	Plan k level1	200	279	39	318	241.51	5.347	75.617	5717.881	-1.015	.172	.021	.342
	Plan k level2	200	1391	705	2095	1569.45	26.003	367.732	135226.642	-.231	.172	-1.009	.342
	Valid N (listwise)	200											
.60	Plan k (total)	200	1684	744	2427	1818.99	31.665	447.813	200536.341	-.347	.172	-.913	.342
	Plan k level1	200	283	39	322	243.85	5.483	77.544	6013.134	-.969	.172	-.083	.342
	Plan k level2	200	1400	705	2105	1575.14	26.383	373.107	139209.050	-.219	.172	-1.031	.342
	Valid N (listwise)	200											
.34	Plan k (total)	200	1684	744	2427	1818.99	31.665	447.813	200536.341	-.347	.172	-.913	.342
	Plan k level1	200	283	39	322	243.85	5.483	77.544	6013.134	-.969	.172	-.083	.342
	Plan k level2	200	1400	705	2105	1575.14	26.383	373.107	139209.050	-.219	.172	-1.031	.342
	Valid N (listwise)	200											

Appendix 7 Additional Model Analysis, Tables, and Figures

Descriptive Statistics

attack severity	Mitigation sum	N Statistic	Range Statistic	Minimum Statistic	Maximum Statistic	Mean		Std. Dev. Statistic	Variance Statistic	Skewness		Kurtosis	
						Statistic	Std. Error			Statistic	Std. Error	Statistic	Std. Error
.51	Plan k (total)	600	1699	744	2443	1801.64	17.627	431.772	186426.840	-.338	.100	-.879	.199
	Plan k level1	600	293	39	331	252.19	3.010	73.728	5435.759	-1.110	.100	.367	.199
	Plan k level2	600	1414	705	2119	1549.45	14.808	362.710	131558.836	-.181	.100	-1.042	.199
	Valid N (listwise)	600											
.71	Plan k (total)	600	1699	744	2443	1801.64	17.627	431.772	186426.840	-.338	.100	-.879	.199
	Plan k level1	600	293	39	331	252.19	3.010	73.728	5435.759	-1.110	.100	.367	.199
	Plan k level2	600	1414	705	2119	1549.45	14.808	362.710	131558.836	-.181	.100	-1.042	.199
	Valid N (listwise)	600											
1.31	Plan k (total)	600	1699	744	2443	1785.21	17.904	438.565	192339.357	-.306	.100	-.937	.199
	Plan k level1	600	291	39	330	248.36	3.058	74.915	5612.280	-1.023	.100	.154	.199
	Plan k level2	600	1414	705	2119	1536.85	15.012	367.714	135213.578	-.160	.100	-1.072	.199
	Valid N (listwise)	600											
3.31	Plan k (total)	600	1699	744	2443	1785.21	17.904	438.565	192339.357	-.306	.100	-.937	.199
	Plan k level1	600	291	39	330	248.36	3.058	74.915	5612.280	-1.023	.100	.154	.199
	Plan k level2	600	1414	705	2119	1536.85	15.012	367.714	135213.578	-.160	.100	-1.072	.199
	Valid N (listwise)	600											
80	1.51 Plan k (total)	400	1684	744	2427	1813.79	21.472	429.446	184423.504	-.353	.122	-.858	.243
	Plan k level1	400	288	39	327	254.69	3.751	75.020	5628.042	-1.143	.122	.384	.243
	Plan k level2	400	1400	705	2105	1559.10	17.976	359.522	129255.816	-.187	.122	-1.030	.243
	Valid N (listwise)	400											
1.54	Plan k (total)	400	1684	744	2427	1813.79	21.472	429.446	184423.504	-.353	.122	-.858	.243
	Plan k level1	400	288	39	327	254.69	3.751	75.020	5628.042	-1.143	.122	.384	.243
	Plan k level2	400	1400	705	2105	1559.10	17.976	359.522	129255.816	-.187	.122	-1.030	.243
	Valid N (listwise)	400											
1.71	Plan k (total)	400	1684	744	2427	1813.79	21.472	429.446	184423.504	-.353	.122	-.858	.243
	Plan k level1	400	288	39	327	254.69	3.751	75.020	5628.042	-1.143	.122	.384	.243
	Plan k level2	400	1400	705	2105	1559.10	17.976	359.522	129255.816	-.187	.122	-1.030	.243
	Valid N (listwise)	400											
1.74	Plan k (total)	400	1684	744	2427	1813.79	21.472	429.446	184423.504	-.353	.122	-.858	.243
	Plan k level1	400	288	39	327	254.69	3.751	75.020	5628.042	-1.143	.122	.384	.243
	Plan k level2	400	1400	705	2105	1559.10	17.976	359.522	129255.816	-.187	.122	-1.030	.243
	Valid N (listwise)	400											

Appendix 7 Additional Model Analysis, Tables, and Figures

Descriptive Statistics

attack severity	Mitigation sum	N Statistic	Range Statistic	Minimum Statistic	Maximum Statistic	Mean		Std. Dev. Statistic	Variance Statistic	Skewness		Kurtosis	
						Statistic	Std. Error			Statistic	Std. Error	Statistic	Std. Error
3.51	Plan k (total)	400	1684	744	2427	1813.79	21.472	429.446	184423.504	-.353	.122	-.858	.243
	Plan k level1	400	288	39	327	254.69	3.751	75.020	5628.042	-1.143	.122	.384	.243
	Plan k level2	400	1400	705	2105	1559.10	17.976	359.522	129255.816	-.187	.122	-1.030	.243
	Valid N (listwise)	400											
	Plan k (total)	400	1684	744	2427	1813.79	21.472	429.446	184423.504	-.353	.122	-.858	.243
	Plan k level1	400	288	39	327	254.69	3.751	75.020	5628.042	-1.143	.122	.384	.243
	Plan k level2	400	1400	705	2105	1559.10	17.976	359.522	129255.816	-.187	.122	-1.030	.243
	Valid N (listwise)	400											
	Plan k (total)	400	1684	744	2427	1813.79	21.472	429.446	184423.504	-.353	.122	-.858	.243
	Plan k level1	400	288	39	327	254.69	3.751	75.020	5628.042	-1.143	.122	.384	.243
	Plan k level2	400	1400	705	2105	1559.10	17.976	359.522	129255.816	-.187	.122	-1.030	.243
	Valid N (listwise)	400											
1.00	Plan k (total)	1200	1722	744	2465	1782.98	12.518	433.650	188052.207	-.324	.071	-.902	.141
	Plan k level1	1200	289	39	328	247.97	2.126	73.661	5425.918	-1.070	.071	.245	.141
	Plan k level2	1200	1433	705	2138	1535.01	10.511	364.107	132573.715	-.172	.071	-1.038	.141
	Valid N (listwise)	1200											
	Plan k (total)	1200	1722	744	2465	1785.61	12.537	434.305	188620.750	-.325	.071	-.896	.141
	Plan k level1	1200	289	39	328	248.92	2.127	73.679	5428.534	-1.072	.071	.262	.141
	Plan k level2	1200	1433	705	2138	1536.69	10.528	364.698	133004.959	-.172	.071	-1.034	.141
	Valid N (listwise)	1200											
	Plan k (total)	1200	1722	744	2465	1782.98	12.518	433.650	188052.207	-.324	.071	-.902	.141
	Plan k level1	1200	289	39	328	247.97	2.126	73.661	5425.918	-1.070	.071	.245	.141
	Plan k level2	1200	1433	705	2138	1535.01	10.511	364.107	132573.715	-.172	.071	-1.038	.141
	Valid N (listwise)	1200											
	Plan k (total)	1200	1722	744	2465	1785.61	12.537	434.305	188620.750	-.325	.071	-.896	.141
	Plan k level1	1200	289	39	328	248.92	2.127	73.679	5428.534	-1.072	.071	.262	.141
	Plan k level2	1200	1433	705	2138	1536.69	10.528	364.698	133004.959	-.172	.071	-1.034	.141
	Valid N (listwise)	1200											

Appendix 7 Additional Model Analysis, Tables, and Figures

Descriptive Statistics

attack severity	Mitigation sum	Descriptive Statistics											
		N Statistic	Range Statistic	Minimum Statistic	Maximum Statistic	Mean Statistic	Std. Error	Std. Dev. Statistic	Variance Statistic	Skewness Statistic	Std Error	Kurtosis Statistic	Std. Error
.51	Plan k (total)	1000	1731	744	2474	1786.90	14.174	448.227	200907.326	-.270	.077	-1.000	.155
	Plan k level1	1000	291	39	330	250.75	2.284	72.241	5218.819	-1.091	.077	.394	.155
	Plan k level2	1000	1440	705	2145	1536.15	12.026	380.299	144627.279	-.118	.077	-1.147	.155
	Valid N (listwise)	1000											
.53	Plan k (total)	1000	1731	744	2474	1786.90	14.174	448.227	200907.326	-.270	.077	-1.000	.155
	Plan k level1	1000	291	39	330	250.75	2.284	72.241	5218.819	-1.091	.077	.394	.155
	Plan k level2	1000	1440	705	2145	1536.15	12.026	380.299	144627.279	-.118	.077	-1.147	.155
	Valid N (listwise)	1000											
.71	Plan k (total)	1000	1731	744	2474	1787.19	14.204	449.156	201741.413	-.264	.077	-1.003	.155
	Plan k level1	1000	291	39	330	251.43	2.288	72.363	5236.364	-1.095	.077	.410	.155
	Plan k level2	1000	1440	705	2145	1535.76	12.054	381.188	145303.980	-.110	.077	-1.149	.155
	Valid N (listwise)	1000											
.73	Plan k (total)	1000	1699	744	2443	1785.94	14.077	445.165	198171.623	-.291	.077	-.991	.155
	Plan k level1	1000	285	39	324	248.12	2.253	71.256	5077.399	-1.106	.077	.392	.155
	Plan k level2	1000	1414	705	2119	1537.82	11.949	377.862	142779.855	-.146	.077	-1.144	.155
	Valid N (listwise)	1000											
1.31	Plan k (total)	600	1670	744	2413	1794.42	16.919	414.436	171757.388	-.415	.100	-.763	.199
	Plan k level1	600	286	39	325	248.99	3.038	74.425	5539.149	-1.110	.100	.290	.199
	Plan k level2	600	1391	705	2095	1545.43	14.074	344.730	118838.794	-.251	.100	-.926	.199
	Valid N (listwise)	600											
1.33	Plan k (total)	400	1670	744	2413	1802.78	21.559	431.173	185910.576	-.395	.122	-.842	.243
	Plan k level1	400	279	39	318	240.96	3.754	75.086	5637.851	-1.021	.122	.029	.243
	Plan k level2	400	1391	705	2095	1561.82	17.943	358.869	128787.166	-.264	.122	-.973	.243
	Valid N (listwise)	400											
3.31	Plan k (total)	400	1670	744	2413	1802.78	21.559	431.173	185910.576	-.395	.122	-.842	.243
	Plan k level1	400	279	39	318	240.96	3.754	75.086	5637.851	-1.021	.122	.029	.243
	Plan k level2	400	1391	705	2095	1561.82	17.943	358.869	128787.166	-.264	.122	-.973	.243
	Valid N (listwise)	400											
3.33	Plan k (total)	500	1670	744	2413	1801.64	19.014	425.171	180769.988	-.393	.109	-.821	.218
	Plan k level1	500	293	39	331	245.99	3.356	75.034	5630.152	-1.059	.109	.164	.218
	Plan k level2	500	1391	705	2095	1555.65	15.838	354.150	125422.552	-.246	.109	-.973	.218
	Valid N (listwise)	500											

Appendix 7 Additional Model Analysis, Tables, and Figures

Descriptive Statistics

attack severity	Mitigation sum		N	Range	Minimum	Maximum	Mean		Std. Dev.	Variance	Skewness		Kurtosis	
			Statistic	Statistic	Statistic	Statistic	Statistic	Std. Error	Statistic	Statistic	Statistic	Std. Error	Statistic	Std. Error
1.20	.31	Plan k (total)	400	1684	744	2427	1818.99	22.363	447.251	200033.744	-.346	.122	-.916	.243
		Plan k level1	400	283	39	322	243.85	3.872	77.447	5998.064	-.965	.122	-.097	.243
		Plan k level2	400	1400	705	2105	1575.14	18.632	372.639	138860.155	-.218	.122	-1.033	.243
		Valid N (listwise)	400											
	.34	Plan k (total)	400	1684	744	2427	1818.99	22.363	447.251	200033.744	-.346	.122	-.916	.243
		Plan k level1	400	283	39	322	243.85	3.872	77.447	5998.064	-.965	.122	-.097	.243
		Plan k level2	400	1400	705	2105	1575.14	18.632	372.639	138860.155	-.218	.122	-1.033	.243
		Valid N (listwise)	400											
	.51	Plan k (total)	1300	1699	744	2443	1789.24	11.853	427.382	182655.695	-.348	.068	-.876	.136
		Plan k level1	1300	293	39	331	250.26	2.030	73.175	5354.604	-1.113	.068	.363	.136
		Plan k level2	1300	1414	705	2119	1538.98	9.952	358.839	128765.274	-.190	.068	-1.037	.136
		Valid N (listwise)	1300											
	.71	Plan k (total)	1400	1699	744	2443	1784.15	11.487	429.795	184723.467	-.333	.065	-.901	.131
		Plan k level1	1400	293	39	331	249.83	1.971	73.766	5441.393	-1.082	.065	.295	.131
		Plan k level2	1400	1414	705	2119	1534.32	9.635	360.500	129960.486	-.178	.065	-1.054	.131
		Valid N (listwise)	1400											
	1.31	Plan k (total)	1200	1699	744	2443	1782.48	12.568	435.367	189544.505	-.317	.071	-.926	.141
		Plan k level1	1200	291	39	330	248.17	2.158	74.755	5588.318	-1.024	.071	.156	.141
		Plan k level2	1200	1414	705	2119	1534.31	10.524	364.579	132917.689	-.172	.071	-1.064	.141
		Valid N (listwise)	1200											
	3.31	Plan k (total)	1200	1699	744	2443	1782.48	12.568	435.367	189544.505	-.317	.071	-.926	.141
		Plan k level1	1200	291	39	330	248.17	2.158	74.755	5588.318	-1.024	.071	.156	.141
		Plan k level2	1200	1414	705	2119	1534.31	10.524	364.579	132917.689	-.172	.071	-1.064	.141
		Valid N (listwise)	1200											
1.20	.31	Plan k (total)	200	1684	744	2427	1818.99	31.665	447.813	200536.341	-.347	.172	-.913	.342
		Plan k level1	200	283	39	322	243.85	5.483	77.544	6013.134	-.969	.172	-.083	.342
		Plan k level2	200	1400	705	2105	1575.14	26.383	373.107	139209.050	-.219	.172	-1.031	.342
		Valid N (listwise)	200											
	.34	Plan k (total)	200	1684	744	2427	1818.99	31.665	447.813	200536.341	-.347	.172	-.913	.342
		Plan k level1	200	283	39	322	243.85	5.483	77.544	6013.134	-.969	.172	-.083	.342
		Plan k level2	200	1400	705	2105	1575.14	26.383	373.107	139209.050	-.219	.172	-1.031	.342
		Valid N (listwise)	200											

Appendix 7 Additional Model Analysis, Tables, and Figures

Descriptive Statistics

attack severity	Mitigation sum	N Statistic	Range Statistic	Minimum Statistic	Maximum Statistic	Mean		Std. Dev. Statistic	Variance Statistic	Skewness		Kurtosis	
						Statistic	Std. Error			Statistic	Std. Error	Statistic	Std. Error
	.51 Plan k (total)	800	1699	744	2443	1788.19	15.179	429.336	184329.415	-.325	.086	-.888	.173
	Plan k level1	800	293	39	331	252.80	2.632	74.441	5541.457	-1.086	.086	.313	.173
	Plan k level2	800	1414	705	2119	1535.39	12.709	359.470	129218.374	-.164	.086	-1.042	.173
	Valid N (listwise)	800											
	.71 Plan k (total)	800	1699	744	2443	1788.19	15.179	429.336	184329.415	-.325	.086	-.888	.173
	Plan k level1	800	293	39	331	252.80	2.632	74.441	5541.457	-1.086	.086	.313	.173
	Plan k level2	800	1414	705	2119	1535.39	12.709	359.470	129218.374	-.164	.086	-1.042	.173
	Valid N (listwise)	800											
1.31	Plan k (total)	600	1670	744	2414	1784.22	17.833	436.813	190805.674	-.320	.100	-.938	.199
	Plan k level1	600	283	39	321	246.23	2.980	73.005	5329.709	-1.089	.100	.278	.199
	Plan k level2	600	1399	705	2104	1537.99	15.030	368.151	135535.081	-.168	.100	-1.084	.199
	Valid N (listwise)	600											
3.31	Plan k (total)	600	1670	744	2414	1784.22	17.833	436.813	190805.674	-.320	.100	-.938	.199
	Plan k level1	600	283	39	321	246.23	2.980	73.005	5329.709	-1.089	.100	.278	.199
	Plan k level2	600	1399	705	2104	1537.99	15.030	368.151	135535.081	-.168	.100	-1.084	.199
	Valid N (listwise)	600											
1.60	.31 Plan k (total)	600	1684	744	2427	1775.86	17.476	428.063	183238.167	-.346	.100	-.887	.199
	Plan k level1	600	283	39	322	246.13	2.977	72.913	5316.357	-1.092	.100	.286	.199
	Plan k level2	600	1400	705	2105	1529.73	14.666	359.230	129046.358	-.195	.100	-1.033	.199
	Valid N (listwise)	600											
	.33 Plan k (total)	600	1684	744	2427	1775.86	17.476	428.063	183238.167	-.346	.100	-.887	.199
	Plan k level1	600	283	39	322	246.13	2.977	72.913	5316.357	-1.092	.100	.286	.199
	Plan k level2	600	1400	705	2105	1529.73	14.666	359.230	129046.358	-.195	.100	-1.033	.199
	Valid N (listwise)	600											
	.34 Plan k (total)	600	1684	744	2427	1775.86	17.476	428.063	183238.167	-.346	.100	-.887	.199
	Plan k level1	600	283	39	322	246.13	2.977	72.913	5316.357	-1.092	.100	.286	.199
	Plan k level2	600	1400	705	2105	1529.73	14.666	359.230	129046.358	-.195	.100	-1.033	.199
	Valid N (listwise)	600											
	.36 Plan k (total)	600	1684	744	2427	1775.86	17.476	428.063	183238.167	-.346	.100	-.887	.199
	Plan k level1	600	283	39	322	246.13	2.977	72.913	5316.357	-1.092	.100	.286	.199
	Plan k level2	600	1400	705	2105	1529.73	14.666	359.230	129046.358	-.195	.100	-1.033	.199
	Valid N (listwise)	600											

Appendix 7 Additional Model Analysis, Tables, and Figures

Descriptive Statistics

attack severity	Mitigation sum	N Statistic	Range Statistic	Minimum Statistic	Maximum Statistic	Mean		Std. Dev. Statistic	Variance Statistic	Skewness		Kurtosis	
						Statistic	Std. Error			Statistic	Std. Error	Statistic	Std. Error
.51	Plan k (total)	600	1725	744	2469	1779.89	18.060	442.366	195687.336	-.285	.100	-.984	.199
	Plan k level1	600	289	39	328	249.31	2.921	71.550	5119.453	-1.124	.100	.445	.199
	Plan k level2	600	1436	705	2141	1530.58	15.319	375.226	140794.727	-.128	.100	-1.137	.199
	Valid N (listwise)	600											
.53	Plan k (total)	600	1725	744	2469	1781.11	18.162	444.865	197904.569	-.269	.100	-.989	.199
	Plan k level1	600	289	39	328	251.04	2.951	72.279	5224.239	-1.112	.100	.432	.199
	Plan k level2	600	1436	705	2141	1530.07	15.388	376.917	142066.201	-.112	.100	-1.138	.199
	Valid N (listwise)	600											
.71	Plan k (total)	600	1725	744	2469	1779.89	18.060	442.366	195687.336	-.285	.100	-.984	.199
	Plan k level1	600	289	39	328	249.31	2.921	71.550	5119.453	-1.124	.100	.445	.199
	Plan k level2	600	1436	705	2141	1530.58	15.319	375.226	140794.727	-.128	.100	-1.137	.199
	Valid N (listwise)	600											
.73	Plan k (total)	200	1670	744	2414	1794.32	31.832	450.173	202655.456	-.309	.172	-1.010	.342
	Plan k level1	200	271	39	310	245.54	4.888	69.129	4778.887	-1.182	.172	.562	.342
	Plan k level2	200	1399	705	2104	1548.78	27.226	385.033	148250.721	-.166	.172	-1.176	.342
	Valid N (listwise)	200											
1.31	Plan k (total)	200	1610	744	2353	1794.60	29.890	422.712	178685.281	-.438	.172	-.800	.342
	Plan k level1	200	276	39	315	240.41	5.285	74.736	5585.544	-1.036	.172	.070	.342
	Plan k level2	200	1334	705	2038	1554.19	24.787	350.539	122877.870	-.311	.172	-.940	.342
	Valid N (listwise)	200											
1.33	Plan k (total)	200	1610	744	2353	1794.60	29.890	422.712	178685.281	-.438	.172	-.800	.342
	Plan k level1	200	276	39	315	240.41	5.285	74.736	5585.544	-1.036	.172	.070	.342
	Plan k level2	200	1334	705	2038	1554.19	24.787	350.539	122877.870	-.311	.172	-.940	.342
	Valid N (listwise)	200											
3.31	Plan k (total)	200	1610	744	2353	1794.60	29.890	422.712	178685.281	-.438	.172	-.800	.342
	Plan k level1	200	276	39	315	240.41	5.285	74.736	5585.544	-1.036	.172	.070	.342
	Plan k level2	200	1334	705	2038	1554.19	24.787	350.539	122877.870	-.311	.172	-.940	.342
	Valid N (listwise)	200											
3.33	Plan k (total)	200	1610	744	2353	1794.60	29.890	422.712	178685.281	-.438	.172	-.800	.342
	Plan k level1	200	276	39	315	240.41	5.285	74.736	5585.544	-1.036	.172	.070	.342
	Plan k level2	200	1334	705	2038	1554.19	24.787	350.539	122877.870	-.311	.172	-.940	.342
	Valid N (listwise)	200											

Appendix 7 Additional Model Analysis, Tables, and Figures

Descriptive Statistics

attack severity	Mitigation sum		N	Range	Minimum	Maximum	Mean		Std. Dev.	Variance	Skewness		Kurtosis	
			Statistic	Statistic	Statistic	Statistic	Statistic	Std. Error	Statistic	Statistic	Statistic	Std. Error	Statistic	Std. Error
1.80	.31	Plan k (total)	600	1684	744	2427	1818.99	18.251	447.065	199866.771	-.346	.100	-.917	.199
		Plan k level1	600	283	39	322	243.85	3.160	77.415	5993.057	-.964	.100	-.102	.199
		Plan k level2	600	1400	705	2105	1575.14	15.207	372.484	138744.245	-.217	.100	-1.034	.199
		Valid N (listwise)	600											
	.34	Plan k (total)	600	1684	744	2427	1818.99	18.251	447.065	199866.771	-.346	.100	-.917	.199
		Plan k level1	600	283	39	322	243.85	3.160	77.415	5993.057	-.964	.100	-.102	.199
		Plan k level2	600	1400	705	2105	1575.14	15.207	372.484	138744.245	-.217	.100	-1.034	.199
		Valid N (listwise)	600											
	.51	Plan k (total)	1900	1699	744	2443	1784.39	9.877	430.511	185339.982	-.338	.056	-.905	.112
		Plan k level1	1900	293	39	331	248.48	1.685	73.432	5392.286	-1.082	.056	.288	.112
		Plan k level2	1900	1414	705	2119	1535.90	8.293	361.475	130664.458	-.186	.056	-1.058	.112
		Valid N (listwise)	1900											
	.71	Plan k (total)	1900	1699	744	2443	1785.78	9.849	429.301	184299.313	-.347	.056	-.891	.112
		Plan k level1	1900	293	39	331	249.41	1.678	73.145	5350.178	-1.100	.056	.332	.112
		Plan k level2	1900	1414	705	2119	1536.38	8.270	360.476	129942.727	-.192	.056	-1.047	.112
		Valid N (listwise)	1900											
	1.31	Plan k (total)	1800	1699	744	2443	1780.92	10.209	433.111	187584.725	-.331	.058	-.924	.115
		Plan k level1	1800	291	39	330	246.70	1.731	73.433	5392.463	-1.067	.058	.238	.115
		Plan k level2	1800	1414	705	2119	1534.22	8.575	363.827	132369.887	-.183	.058	-1.070	.115
		Valid N (listwise)	1800											
	3.31	Plan k (total)	1800	1699	744	2443	1780.92	10.209	433.111	187584.725	-.331	.058	-.924	.115
		Plan k level1	1800	291	39	330	246.70	1.731	73.433	5392.463	-1.067	.058	.238	.115
		Plan k level2	1800	1414	705	2119	1534.22	8.575	363.827	132369.887	-.183	.058	-1.070	.115
		Valid N (listwise)	1800											
2.40	.31	Plan k (total)	200	1684	744	2427	1818.99	31.665	447.813	200536.341	-.347	.172	-.913	.342
		Plan k level1	200	283	39	322	243.85	5.483	77.544	6013.134	-.969	.172	-.083	.342
		Plan k level2	200	1400	705	2105	1575.14	26.383	373.107	139209.050	-.219	.172	-1.031	.342
		Valid N (listwise)	200											
	.34	Plan k (total)	200	1684	744	2427	1818.99	31.665	447.813	200536.341	-.347	.172	-.913	.342
		Plan k level1	200	283	39	322	243.85	5.483	77.544	6013.134	-.969	.172	-.083	.342
		Plan k level2	200	1400	705	2105	1575.14	26.383	373.107	139209.050	-.219	.172	-1.031	.342
		Valid N (listwise)	200											

Appendix 7 Additional Model Analysis, Tables, and Figures

Descriptive Statistics

attack severity	Mitigation sum	N Statistic	Range Statistic	Minimum Statistic	Maximum Statistic	Mean		Std. Dev. Statistic	Variance Statistic	Skewness		Kurtosis	
						Statistic	Std. Error			Statistic	Std. Error	Statistic	Std. Error
.51	Plan k (total)	600	1670	744	2414	1781.02	17.511	428.926	183977.480	-.358	.100	-.893	.199
	Plan k level1	600	283	39	322	247.58	2.962	72.559	5264.805	-1.112	.100	.347	.199
	Plan k level2	600	1399	705	2104	1533.44	14.717	360.479	129945.430	-.205	.100	-1.050	.199
	Valid N (listwise)	600											
.71	Plan k (total)	600	1670	744	2414	1778.77	17.583	430.705	185506.722	-.345	.100	-.916	.199
	Plan k level1	600	283	39	321	245.87	2.969	72.729	5289.486	-1.096	.100	.296	.199
	Plan k level2	600	1399	705	2104	1532.90	14.785	362.165	131163.815	-.196	.100	-1.069	.199
	Valid N (listwise)	600											
1.31	Plan k (total)	600	1670	744	2414	1778.77	17.583	430.705	185506.722	-.345	.100	-.916	.199
	Plan k level1	600	283	39	321	245.87	2.969	72.729	5289.486	-1.096	.100	.296	.199
	Plan k level2	600	1399	705	2104	1532.90	14.785	362.165	131163.815	-.196	.100	-1.069	.199
	Valid N (listwise)	600											
3.31	Plan k (total)	600	1670	744	2414	1778.77	17.583	430.705	185506.722	-.345	.100	-.916	.199
	Plan k level1	600	283	39	321	245.87	2.969	72.729	5289.486	-1.096	.100	.296	.199
	Plan k level2	600	1399	705	2104	1532.90	14.785	362.165	131163.815	-.196	.100	-1.069	.199
	Valid N (listwise)	600											
4.80	3.76 Plan k (total)	1600	3096	734	3830	3247.07	19.913	796.527	634454.557	-1.576	.061	1.521	.122
	Plan k level1	1600	349	39	388	337.48	2.121	84.841	7197.968	-2.069	.061	3.276	.122
	Plan k level2	1600	2750	695	3444	2909.59	17.841	713.620	509253.943	-1.512	.061	1.314	.122
	Valid N (listwise)	1600											

Appendix 8 Lists of Tables, Figures, Equations and Acronyms

List of Tables

Table 1: Three primary sets of deliverables.....	10
Table 2: Three observations on organizational learning.....	19
Table 3: Structural challenges to organizational learning.....	20
Table 4: CNSSI 4009 definitions of CIAAN.....	22
Table 5: DoD definitions of the five D's (2006)	23
Table 6: Descriptive statistics of citations collected for literature review.....	35
Table 7: Nine (9) node metanetwork and their internode link interpretations.....	61
Table 8: Common SNA metrics and their interpretations	62
Table 9: Number of input files per model.....	82
Table 10: File sizes descriptives per model/level of war – part 1	82
Table 11: File sizes (MB) descriptives per model/level of war – part 2.....	82
Table 12: Size of D2M wizard generated <i>suggested ngrams</i> list and <i>possible acronyms</i> list	83
Table 13: Quantities of D2M wizard generated concepts as <i>ngrams</i> and <i>singletons</i> drawn from the union of generated <i>concept lists</i>	83
Table 14: Metanetwork link descriptives for D2M cycle 0	84
Table 15: Metanetwork entities per ontological category for D2M cycle 0	84
Table 16: <i>Concept list</i> entities per ontological category for D2M cycle 0	86
Table 17: <i>finalThesaurus</i> entities per ontological category D2M cycle 0	86
Table 18: Three (3) terminating conditions for D2M process	87
Table 19: Count per ontological category for each of the final thesauri (cycle 12 and higher)	89
Table 20: Metanetwork entities per ontological category (cycle 12 and higher)	89
Table 21: Metanetwork descriptives (cycle 12 and higher).....	89
Table 22: Counts of N-grams, singletons, acronyms, nonacronyms (cycle 12 and higher) ...	89
Table 23: IT related agents and resources in all three generated models (cycle 12 and higher)	91
Table 24: Visualization options for organization x organization Models.....	110
Table 25: A sample of metanetwork measures for indicators of resilience.....	122
Table 26: Dissertation measures of interest (MoI)	133
Table 27: Descriptive statistics for D2M resilience scores.....	135
Table 28: Descriptive statistics for D2M characteristic path length.....	135
Table 29: Descriptive statistics for D2M congruence, organization, agent knowledge needs	136
Table 30: Descriptive statistics for D2M congruence, organization, agent knowledge waste	136
Table 31: Descriptive statistics for D2M congruence, organization, [agent IT agent] [resource IT resource] needs, baseline	137
Table 32: Descriptive Statistics for D2M congruence, organization, [agent IT agent] [resource IT resource] waste, baseline	138
Table 33: Descriptive Statistics for D2M congruence, organization, task knowledge needs, baseline	140
Table 34: Descriptive Statistics for D2M congruence, organization, task knowledge waste	141

Appendix 8 Lists of Tables, Figures, Equations, and Acronyms

Table 35: Descriptive statistics for D2M congruence, organization, [agent IT agent] [resource IT resource] waste, baseline	141
Table 36: Descriptive statistics for D2M congruence, organization, task [resource IT resource] waste, baseline	142
Table 37: Descriptive statistics for D2M congruence, social technical.....	143
Table 38: Descriptive statistics for D2M density, clustering coefficient.....	143
Table 39: Descriptive statistics for D2M diffusion, baseline	144
Table 40: Descriptive statistics for D2M fragmentation, baseline	145
Table 41: Descriptive statistics for D2M isolate count, baseline.....	146
Table 42: Descriptive statistics for D2M complexity, baseline.....	146
Table 43: Descriptive statistics for D2M performance as accuracy, baseline	147
Table 44: Descriptive statistics for D2M Social Density, Baseline.....	148
Table 45: Descriptive statistics for D2M averageSpeed, Baseline	148
Table 46: Descriptive statistics for D2M Shared Situation Awareness, Baseline	150
Table 47: Interpreting key entity reports as a operational PDAL.....	153
Table 48: Interpreting key entity reports as strategic PDAL	155
Table 49: Operational model nodes to Remove.....	156
Table 50: Strategic Model Nodes to Remove	157
Table 51: Exogenous modifications to D2M models	176
Table 52: Experimental summary for D2M generated models.....	194
Table 53: 10 factor Box-Behnken design	195
Table 54: Lines of code summary for Construct, pre-dissertation.....	199
Table 55: Lines of code summary for Construct, post-dissertation, by Joseph, Kowalchuck and Lanham.....	199
Table 56: Lines of code added and removed during refactoring and additions.....	200
Table 57: Class count changes in code base	202
Table 58: Effects of random losses table	219
Table 59: Rules of thumb for impacts.....	221
Table 60: Descriptive statistics for D2M of Citation Titles.....	2-9
Table 61: Metanetwork ontological labeling heuristics.....	3-9
Table 62: Parameters used to in operational and strategic simulations	5-15
Table 63: Box-Behnken design of six attack vectors and four mitigations	16

List of Figures

Figure 1: Mission assurance is more than risk management	6
Figure 2: Dynamic visualization of resilience for an arbitrary measure of interest (MoI)	7
Figure 3: Federal Communications Commission (FCC) frequency allocation chart circa 2003	12
Figure 4: FCC frequency allocations circa 1975	12
Figure 5: Sales growth for personal computers from 1998 to 2011	13
Figure 6: Growth in installed super-computers by continent since	13
Figure 7: US DoD frequency allocation chart circa 2010	14
Figure 8: Five pillars of IA and the five D's	23
Figure 9: Intuition based clustering and links between clusters of the Literature Corpus.....	34
Figure 10: LSA 6 topics, top 10 members/topic	36

Appendix 8 Lists of Tables, Figures, Equations, and Acronyms

Figure 11: LSA 7 topics, top 10 members/topic	36
Figure 12: LSA 8 topics, top 10 members/topic	36
Figure 13: LSA 9 topics, top 10 members/topic	36
Figure 14: LSA 10 topics, top 10 members/topic	36
Figure 15: LSA 11 topics, top 10 members/topic	36
Figure 16: ORA™ generated LSA analysis of collected citations with 10 topics.....	37
Figure 17: LDA 8 topics, top 10 members/topic	39
Figure 18: LDA 9 topics, top 10 members/topic	39
Figure 19: LDA 10 topics, top 10 members/topic	39
Figure 20: LDA 11 topics, top 10 members/topic	39
Figure 21: LDA 12 topics, top 10 members/topic	39
Figure 22: LDA 13 topics, top 10 members/topic	39
Figure 23: ORA™ generated LDA analysis of collected citations with 13 topics	40
Figure 24: Key entity 'Author'	43
Figure 25: Key entity 'Journal'	43
Figure 26: Key entity 'Publisher'	44
Figure 27: Key entity 'Article'	44
Figure 28: Zoomed in co-authorship network, edges with weight < 2 hidden, zoomed in on prolific author clusters	45
Figure 29: co-authorship network, edges with weight < 3.5 hidden, pendants removed, not zoomed in.....	45
Figure 30: Zoomed in co-authorship network, edges with weight < 3.5 hidden, with pendants removed, zoomed in on prolific authors	45
Figure 31: Zoomed in co-authorship network, edges with weight < 3.5 hidden, with pendants remaining,, zoomed in on prolific authors	46
Figure 32: Co-citation network of article x article, no filtering.....	46
Figure 33: Co-citation network of article x book, no filtering.....	47
Figure 34: Four-node metanetwork	62
Figure 35: Stylized dissertation workflow	71
Figure 36: Dissertation workflow data to model (D2M)	73
Figure 37: Data to model wizard applied to any input corpus	75
Figure 38: D2M refinement applied to DoD input corpus.....	76
Figure 39: Simplified DoD hierarchy--strategic to operational	78
Figure 40: Simplified figure of USG strategic level organizations	79
Figure 41: Simplified figure of COCOM and USAF operational level organizations	80
Figure 42: USAF doctrinal air operations center organizational structure	81
Figure 43: USAF AOC as a text mined model of links and nodes	81
Figure 44: Size of D2M wizard generated ngram list and possible acronym list	83
Figure 45: Quantities of D2M wizard generated concepts as <i>ngram</i> and <i>singletons</i> drawn from the union of generated concept lists	84
Figure 46: Recurring top ranked agents (top 3), operational model	92
Figure 47: Recurring top ranked agents (top 20), operational model	93
Figure 48: Recurring top ranked human agents (top 3), operation model	93
Figure 49: Recurring top ranked human agents (top 20), operational model	94
Figure 50: Recurring top tanked IT agents (top 3), operational model	95
Figure 51: Recurring top ranked IT agents (top 20), operational model	95

Appendix 8 Lists of Tables, Figures, Equations, and Acronyms

Figure 52: Recurring top ranked organizations (top 3), operational model.....	96
Figure 53: Recurring top ranked organizations (top 20), operational model.....	96
Figure 54: Recurring top ranked resources (top 3), operational model	97
Figure 55: Recurring top ranked resources (top 20), operational model	97
Figure 56: Recurring top ranked Non-IT resources (top 3), operational model	98
Figure 57: Recurring top ranked Non-IT resources (top 20), operational model	99
Figure 58: Recurring top ranked IT resources (top 3), operational model	99
Figure 59: Recurring top ranked IT resources (top 20), operational model	100
Figure 60: Recurring top ranked agents (top 3), strategic model	101
Figure 61: Recurring top ranked Agents (top 20), strategic model	102
Figure 62: Recurring top ranked Human Agents (top 3), strategic model.....	103
Figure 63: Recurring top ranked Human Agents (top 20), strategic model.....	103
Figure 64: Recurring top ranked IT agents (top 3), strategic model.....	104
Figure 65: Recurring top ranked IT agents (top 20), strategic model.....	104
Figure 66:: Recurring top ranked Recurring top ranked organizations (top 3), strategic model	105
Figure 67: Recurring top ranked Organizations (top 20), strategic model	106
Figure 68: Recurring top ranked Recurring top ranked resources (top 3), strategic model.	106
Figure 69: Recurring top ranked Recurring top ranked resources (top 20), strategic model	107
Figure 70: Recurring top ranked Non-IT resources (top 3), strategic model.....	108
Figure 71: Recurring top ranked Non-IT resources (top 20), strategic model.....	108
Figure 72: Recurring top ranked IT resources (top 3), strategic model.....	109
Figure 73 Recurring top ranked IT resources (top 20), strategic model.....	109
Figure 74: Node color legend for operational organization x organization visualizations...	111
Figure 75: Operational org x org, no filtering by link weight	111
Figure 76: Operational org x org, filtering by level of warfare \neq blank (the level is unambiguously within scope, exogenously determined by researcher).....	111
Figure 77: Operational org x org, filtering by link weight ≥ 15	111
Figure 78: Operational org x org, filtering by link weight ≥ 35	112
Figure 79: Node color legend for strategic organization x organization visualizations	112
Figure 80: Strategic org x org, no filtering by link weight	112
Figure 81: Strategic org x org, filtering by link weight ≥ 15	113
Figure 82: Strategic org x org, filtering by level of warfare \neq blank (the level is unambiguously within scope, exogenously determined by researcher).....	113
Figure 83: Strategic org x org, filtering by link weight ≥ 35	113
Figure 84: Dissertation workflow static analysis prior to augmentation for agent based modeling	119
Figure 85: Dynamic visualization of resilience for an arbitrary measure of interest (MoI) .	119
Figure 86: 2D projection of 3D rendering of two access indices	126
Figure 87: Sigmoid function of knowledge + resource needs component, low input values best	127
Figure 88: Sigmoid function of Knowledge + Resource Waste Component, high input values best	129
Figure 89: 2D rendering of resilience score, as function of access indices, wastes, and needs	131

Appendix 8 Lists of Tables, Figures, Equations, and Acronyms

Figure 90: Surface mapping of interaction between a single waste and a single needs/access value	131
Figure 91: 3D surface rendering of theoretical resilience scores, as function of access indices, wastes, and needs	132
Figure 92: congruenceOrg[agent IT agent] [resource IT resource] needs score	137
Figure 93: congruenceOrg[agent IT agent][resource IT resource] waste, baseline	137
Figure 94: congruenceOrgTaskKnowledgeNeeds, Baseline	140
Figure 95: congruenceOrgTaskKnowledgeWaste, Baseline	140
Figure 96: congruenceOrgTaskResource needs, baseline	142
Figure 97: congruenceOrgTaskResource waste, baseline	142
Figure 98: clusteringCoefficient needs, baseline	144
Figure 99: diffusion [it]agent itresource], baseline	144
Figure 100: Fragmentation, baseline	145
Figure 101: isolateCount [[IT]sgent resource], baseline	145
Figure 102: performanceAsAccuracy, baseline	147
Figure 103 Social Density, Baseline	148
Figure 104: averageSpeed, baseline	149
Figure 105: Shared situation awareness (agent and IT agent), baseline	149
Figure 106: Resilience score for entropic and targeted deletions	158
Figure 107: Changes in characteristic path length of IT agents for entropic and targeted deletions	159
Figure 108: Changes in communication speed of IT agents for entropic and targeted deletions	159
Figure 109: Changes in clustering coefficient of IT agents for entropic and targeted deletions	160
Figure 110: Changes in diffusion of IT agents for entropic and targeted deletions	161
Figure 111: Changes in fragmentation of IT agents for entropic and targeted deletions	161
Figure 112: Change in isolate count of IT agents for entropic and targeted deletions	162
Figure 113: Overall changes in complexity	163
Figure 114: Change in social density of IT agents	163
Figure 115: Changes in performance as accuracy of agents	164
Figure 116: Changes to performance as accuracy of roles	165
Figure 117: Changes to performance as accuracy of IT agents	166
Figure 118: Dissertation workflow augmentation of models for use in ABM	175
Figure 119: Knowledge x knowledgegroup network	178
Figure 120: Agent x Communications Medium (Operational)	183
Figure 121: Shared planning knowledge	189
Figure 122 Graphical representation of organization under test	192
Figure 123: Graphical rendering of experimental setup with factor tree and Box-Behnken leaves	194
Figure 124: Visual representation of distribution of sums of attack probabilities and mitigations' values	196
Figure 125 Dissertation workflow executing simulations of models	198
Figure 126: 'Plan' diffusion for operational model	205
Figure 127: Operational model information diffusion effects for single-vector and multi-vector attack conditions	206

Appendix 8 Lists of Tables, Figures, Equations, and Acronyms

Figure 128: Strategic model best and worst cases only	208
Figure 129: Baseline performance as accuracy for operational model	209
Figure 130: Baseline reflection of performance as accuracy for strategic model	210
Figure 131: Average plan distribution across attack and mitigation conditions	211
Figure 132: Confidentiality sink's collection of various knowledge groups	212
Figure 133: Operational model information diffusion effects for single-vector and multi- vector attack conditions	214
Figure 134: USAF Visual Depiction of Mission Assurance (Elder, 2008)	1-3
Figure 135: Dynamic visualization of resilience for an arbitrary measure of interest (MoI)(Morgan & Lanham, 2012)	1-5
Figure 136: Dynamic visualization of resilience for an arbitrary measure of organization (MoO)(Morgan & Lanham, 2012)	1-7
Figure 137: Data-to-Model (D2M) User Interface of AutoMap	2-8
Figure 138: Concept x TFIDF	2-9
Figure 139: TFIDF x Cumulative Percentage of Σ TFIDF	2-10
Figure 140: Directory structure for virtual experiments	4-2
Figure 141: Directory structure for construct within virtual experiment directory structure	4-2
Figure 142: Snapshot of params_template.xls, Columns A-H	4-4
Figure 143: Snapshot params_templat.xls, Columns E-J	4-5
Figure 144: Snapshot of experiment_config_file.xls	4-7
Figure 145: Directory structure for construct runs	4-9
Figure 146: Eclipse's Run configurations menu item	4-11
Figure 147: Eclipse run configuration for NetworkDataAggregator – main tab	4-12
Figure 148: Eclipse run configuration for NetworkDataAggregator – arguments tab	4-12

List of Equations

Equation 1: Risk as a function of the probability of occurrence and the forecasted impact ..	24
Equation 2: Risk as a function of three variables: threat nature, vulnerability nature, and asset value	24
Equation 3: Node set definition in set notation	41
Equation 4: Edge set definition in set notation	41
Equation 5: Measures set definition in set notation	41
Equation 6: A measure's output definition in set notation	41
Equation 7: A set of maximum values from a measure's output in set notation	41
Equation 8: A set of node identifiers corresponding to maximum values from a single measure in set notation	41
Equation 9: A set of measures' results as sets of node identifiers in set notation	42
Equation 10: Calculating the frequency of occurrence a node is in the maximum value set of all relevant measures	42
Equation 11: A set of maximum frequency of occurrence values in set notation	42
Equation 12: A set of node identifiers corresponding to maximum frequency of occurrence values in set notation	42
Equation 13: Resilience as a function of the magnitude of transformation, the frequency of transformation, time, expense, and emotional energy	56
Equation 14: Structural resilience as a new metanetwork calculation	124

Appendix 8 Lists of Tables, Figures, Equations, and Acronyms

Equation 15: Access index as reflection of criticality through near isolation (Kathleen M. Carley, Juergen Pfeffer, et al., 2012)	124
Equation 16: Normalized summation of a model's knowledge access index, agents aggregated	124
Equation 17: Knowledge access component sigmoid, right shifted six values, in 12 bins...	125
Equation 18: Normalized summation of a model's knowledge access index, agents disaggregated	125
Equation 19: Knowledge access component sigmoid, right shifted six values, in 12 bins, agents disaggregated	125
Equation 20: Normalized summation of a model's task access index, agents disaggregated	125
Equation 21: Normalized summation of a model's resource and IT resource access index, agents disaggregated	125
Equation 22: Access Index Component, adjusted for disaggregation of Agent and Resource node sets.....	125
Equation 23: Tasks with needed knowledge via assigned agents (Kathleen M. Carley, Juergen Pfeffer, et al., 2012).....	127
Equation 24: Percentage of knowledge not provided by agents assigned to tasks (Knowledge Needs) (Kathleen M. Carley, Juergen Pfeffer, et al., 2012).....	127
Equation 25: Knowledge needs, right shifted 6 values, in 12 bins	127
Equation 26: Needs Component as sum of two sigmoid needs functions, right shifted 6 values, in 12 bins.....	127
Equation 27: <i>congruenceOrgTaskKnowledgeNeeds</i> with disaggregated agents and IT agents (Kathleen M. Carley, Juergen Pfeffer, et al., 2012).....	127
Equation 28: Tasks with needed resources via assigned agents (Kathleen M. Carley, Juergen Pfeffer, et al., 2012)	127
Equation 29: Percentage of resources not provided by agents assigned to tasks (Kathleen M. Carley, Juergen Pfeffer, et al., 2012)	128
Equation 30: Resource needs, right shifted 6 values, in 12 bins.....	128
Equation 31: <i>congruenceOrgTaskResourceNeeds</i> with disaggregated agents and IT agents (Kathleen M. Carley, Juergen Pfeffer, et al., 2012).....	128
Equation 32: Percentage of knowledge not used for tasks assigned to agents (Kathleen M. Carley, Juergen Pfeffer, et al., 2012)	129
Equation 33 Knowledge waste, right shifted 6 values, in 12 bins	129
Equation 34: <i>congruenceOrgTaskKnowledgeWaste</i> with disaggregated agents and IT agents (Kathleen M. Carley, Juergen Pfeffer, et al., 2012).....	129
Equation 35: Percentage of resources not used for tasks assigned to agents (Kathleen M. Carley, Juergen Pfeffer, et al., 2012)	129
Equation 36: Resource 'Waste,' right shifted 6 values, in 12 bins	130
Equation 37: <i>congruenceOrgTaskResourceNeeds</i> with disaggregated agents and IT agents (Kathleen M. Carley, Juergen Pfeffer, et al., 2012).....	130
Equation 38: Waste Component as sum of two sigmoid waste functions, right shifted 6 values, in 12 bins.....	130
Equation 39 agent x agent probability of interaction.....	182
Equation 40: Law of Cosines to calculate distances between two points on a sphere.....	189
Equation 41: Generating an agent x location network (count of shared organization)	190

Appendix 8 Lists of Tables, Figures, Equations, and Acronyms

Equation 42: Generating an agent x location network (sum of distances between ego instances).....	190
Equation 43: Generating an agent x agent network (count of shared locations)	190
Equation 44: Generating an agent x agent (sum of distances between egos and alters).....	190
Equation 45: Generating average distance between ego and alter agents	191
Equation 46: Generating an agent x agent physical proximity network for use by Construct, scale [1.0,0.0].....	191
Equation 47: Naive experimental design and summary	195
Equation 48: Box-Behnken experimental design and summary	196
Equation 49: Term Frequency for Concept x	2-8
Equation 50: Inverse Document Frequency for Term x in Corpus	2-9
Equation 51: Term Frequency x Inverse Document Frequency (TFIDF)	2-9

Acronyms

ABM	agent based model / agent based modeling
ACOA	automated courses of action
ADA	air defense artillery
AFI	Air Force Instruction
AI	artificial intelligence
ADP	automated data process
ANSI	American National Standards Institute
AOC	Air Operations Center
APT	Advanced persistent threat
BLOS	beyond line of sight
CAOC	Coalition Air Operations Center
CARVER	Criticality, Accessibility, Recuperability, Vulnerability, Effect and Recognizability
CAS	complex adaptive systems
CASOS	Center for Computational Analysis of Social and Organizational Systems
CDC	Center for Disease Control
CDS	cross domain solution
CENTRIX	Combined Enterprise Regional Information Exchange
CEO	Chief Executive Office
CIA	confidentiality, integrity, availability
CIAAN	confidentiality, integrity, availability, authentication, non-repudiation
CJCS	Chairman of the Joint Chiefs of Staff
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CJFACC	Combined Joint Force Air Component Commander
CMU	Carnegie Mellon University
CNA	computer network attack, see also OCO
CNSS	Committee on National Security Systems
CNSSI	Committee on National Security Systems Instruction
COMPUSEC	computer security
COCOM	combatant command
COP	common operating picture
CVE	common vulnerability exposure

Appendix 8 Lists of Tables, Figures, Equations, and Acronyms

D2M	data to model
DDoS	distributed denial of service
DHS	Department of Homeland Security
DIRNSA	Director National Security Agency
DSCS	Defense Satellite Communications System
DMU	decision making unit
DNA	dynamic network analysis
DNI	Director National Intelligence
DoD	Department of Defense
DoDD	Department of Defense Directive
DOS	denial of service
EBO	effects based operations
EECS	Electrical Engineering and Computer Science
ERM	Enterprise Risk Management
ETF	exchange traded funds
FAA	Federal Aviation Authority
FCC	Federal Communications Commission
FISMA	Federal Information Security Management Act
FFRDC	Federally Funded Research and Development Corporation
GAMES	Global Air Mobility Support System
GCC	geographical combatant command
GCCS	Global Command and Control System
GPS	global positioning system
HR	human resources
HRO	high reliability organization
HSPD	Homeland Security Presidential Directive
IA	information assurance
IC	intelligence community
IDS	intrusion detection system
INFOSEC	information security
IPS	intrusion protection system / intrusion prevention system
IRC	internet relay chat
ISO	Institute Organization of Standards
ISR	intelligence, surveillance, reconnaissance
IT	information technology
IW	information warfare
JCS	Joint Chiefs of Staff
JOPEs	Joint Operations Planning and Execution System
JP	Joint Publication
JPG	joint planning group
JWICS	Joint Worldwide Intelligence Communications System
LDA	Latent Dirichlet allocation
LIMFAC	limiting factor
LOS	line of sight
LSA	latent semantic analysis
M&S	modeling and simulation

Appendix 8 Lists of Tables, Figures, Equations, and Acronyms

MDMP	military decision making process
MILDEC	military deception
MILDEP	military department
MoE	measure of effectiveness
MoI	measure of interest
MoP	measures of performance
MSE	mobile subscriber equipment
NAF	numbered Air Force
NCA	national command authority
NIST	National Institute of Standards and Technology
NMCI	Navy/Marine Corps Intranet
NSC	National Security Council
OCO	offensive cyber operations, replaces CNA
OGA	other governmental agencies
OPORD	operations order
ORA	Organization Risk Analyzer, deprecated to just CASOS
PaA	performance as accuracy
PDF	portable document format
POP	point of presence
POTUS	President of the United States
RBV	resource-based view
RF	radio frequency
RINSE	Real-Time Immersive Network Simulation Environment
SCADA	supervisory control and data acquisition
SCM	supply chain management
SECDEF	Secretary of Defense
SEI	Software Engineering Institute
SME	subject matter expert
SNA	social network analysis
SOF	special operations forces
SOP	standard operating procedures
SPOF	single point of failure
SSA	Shared Situational Awareness
SVD	single value decomposition
TBMCS	theater battle management core system
TELCO	telecommunications company
UAV	unmanned aerial vehicle
USAF	United States Air Force
USAFCENT	US Air Force Central Command
USCC	United States Cyber Command
USCENTCOM	United States Central Command
USCYBERCOM	United States Cyber Command, see also USCC
USB	universal serial bus
USD	US dollar
USG	United States Government
USMA	United States Military Academy

Appendix 8 Lists of Tables, Figures, Equations, and Acronyms

USSTRATCOM	US Strategic Command
USTRANSCOM	US Transportation Command
WHO	World Health Organization
WWII	World War II

Appendix 9 Index

ACOA	62	nonrepudiation	26
acronyms	83	replay	25
Act		authentication	4, 8, 20, 167, 168, 169, 170, 1-9, 3-1
Goldwater-Nichols	85	AutoMap	81
adaptability		availability	vii, 2, 4, 8, 10, 17, 20, 25, 29, 34, 53, 57, 60, 99, 115, 182, 189, 203, 205, 208, 242, 1-2, 1-5, 1-9
perception	19, 23, 61	Availability	4, 130, 211
adaptable	22	avoidance	27, 28, 52
adaptation	6, 19, 21, 24, 36, 42, 60, 62, 63, 64, 65, 74, 81, 130, 187, 189, 224, 233, 242, 1-7, 1-8, 2-2	risk	52
adversary	4, 5, 8, 10, 17, 27, 29, 99, 100, 166, 203, 204, 241, 242, 3-11	back-citation	37
Dolev & Yao	29	balance	57
incompetent	23	battle damage assessment	171
agent		BDA	<i>See</i> battle damage assessment
confidentiality	5, 193	Behavioral psychologists	22
integrity	5	behaviors	5, 61, 186
key IT	185, 193, 198	Boost	219
Air Force		business continuity	37, 58, 75
United States	6	Carley, Kathleen M.	v
US	v, 23, 88, 107	Carnegie Mellon University	37, 188
ambiguous	63, 119	CARVER	132, 166
analysis		CASOS	v, 37, 68, 81, 83, 91, 93, 95, 125, 189, 250, 2-1, 2-8, 2-12, 3-1
network	38, 75, 100, 132	Center for Computational Analysis of Social and Organizational Systems	v, 37
semantic	37, 80	CIA	9, 57, 130, 1-5, 1-6
semantic network	75	CIAAN	8
ANSI	61, 62, 8-8	CJCSI 6510.01F	55
Armed Services	23	Clarke	
Army		Richard	30
US	v, 23	CMU	37, 68, 2-2
assessment		CNA	8, 9, 26, 1-5, 1-8
organizational	65	CNSS	4, 8, 25, 26, 28, 1-1, 1-5
attack		Instruction	25
authentication	25	Co-Citation network	50
availability	11, 25	cognitive	70, 74, 75, 132, 144, 145, 184, 186, 1-7, 3-11
confidentiality	25	command-level	vii, 1, 3, 12
confidentiality	11	Committee of National Security Systems	4, 8
cryptographic	9	compliance	9, 55, 125
cyber	29, 33, 34, 180, 203, 204, 214	COMPUSEC	6, 1-2, 1-3, 1-9
denial of service	9, 25		
distributed denial of service	9		
integrity	25		
message replay	9		

Appendix 9 Index

- computer network attack 8, 26, 1-5
- conditions
 - in extremis 56
 - peak-loading 56
- confidentiality vii, 2, 5, 8, 17, 20, 25, 29, 57, 99, 203, 208, 242, 1-2, 1-5, 1-9
- Confidentiality 4, 130, 211
- configurations
 - structural 5
- congruence
 - communication 70
- Connecticut 32
- Construct 71, 73, 77, 126, 185, 187, 188, 189, 190, 193, 196, 200, 204, 243, 244, 245, 247, 248, 250, 4-4, 4-5
- co-occurrence 92, 119, 201
- COP 103, 167, 169, 171
- crisis management 58
- culture
 - homogeneous 64
- cyber attacks *See* attack, cyber
- cyber environment
 - contested vii, 1, 2, 3, 4, 8, 10, 11, 12, 13, 16, 17, 18, 20, 21, 24, 26, 27, 28, 29, 32, 33, 34, 36, 37, 53, 58, 62, 65, 70, 72, 73, 74, 75, 77, 98, 99, 126, 128, 133, 144, 157, 175, 181, 188, 203, 250, 1-3, 1-4
- cyber risk management 37, 42, 55, 65, 75
- cyberspace 5, 10, 17, 18, 52, 86, 1-1
- cyberspace-enabled 52
- D2M
 - process 78, 80, 81, 82, 83, 88, 91, 93, 95, 105, 106, 114, 119, 125, 160, 185, 193, 196, 197, 198, 200, 201, 221, 240, 244, 245, 250, 2-9, 3-1, 3-12
 - Wizard 81, 85, 89, 90, 91, 92
- DDoS 9, 1-5
- deceive 26
- decision makers 3, 6, 27, 53, 183, 196, 1-2, 1-8
- decision making 5, 68
- Defended Asset List 166
 - Prioritized 166, 167
- degradation 10, 11, 17, 18, 24, 55, 59, 71, 74, 1-2, 1-5, 1-7
- degrade 8, 26, 27, 33, 61, 237, 1-8
- degraded 2, 10, 17, 23, 30, 64, 72, 188, 2-2, 3-12
- denial 9, 10, 17, 25, 34, 59, 71, 1-2, 1-5, 1-7, 1-9
- denial of service 9, 71, 1-5, 1-9
- Density Clustering Coefficient 174
- deny 8, 26, 203, 1-8, 1-9, 3-9, 19
- Department of Defense 8, 15, 25, 113, 114, 125, 188, 3-1, 3-7
- dependencies 2, 58, 68, 70, 74, 131, 145
- destroy 8, 26, 60, 1-8
- destruction 10, 17, 24, 30, 32, 34, 59, 60, 74, 1-5, 1-7
- deterministic 57
- DHS 62, 70
- disaster management 37
- disinformation 5
- disrupt 8, 26, 61, 118, 1-8
- disruption 7, 9, 10, 11, 17, 18, 19, 20, 24, 34, 59, 64, 70, 143, 170, 176, 1-2, 1-5, 1-7
- DNA 65, 128, 249, 250, *See* dynamic network analysis
- doctrine 23, 84, 99, 102, 103, 105, 106, 110, 112, 113, 114, 116, 132, 148, 165, 181, 183, 241, 1-1, 3-5
- DoD 8, 15, 16, 23, 25, 26, 55, 72, 77, 81, 83, 84, 86, 91, 95, 97, 98, 99, 115, 117, 122, 125, 205, 241, 250, 3-1, 3-8
- DODD 8500.01E 55
- doxygen 219
- dynamic network analysis 2, 70, 128
- earthquakes 10
- EBO 21
- EECS v
- effects
 - psychological 36
- effects based operations 21, 8-9
- efficiency 27, 57
- Elder, Robert v
- electronically traded funds 11, 18
- emergency services 10, 17
- empirical 34, 57, 74, 77, 126, 191, 209, 240, 246, 247, 11, 16, 17
- engineering

Appendix 9 Index

resilience	65	IC	197
environment		impact	2, 27, 28, 33, 52, 83, 131, 133, 164, 165, 180, 181, 183, 221, 235, 236, 238, 240, 1-5, 4-5
cyber, contested	1, 5, 8, 10, 11, 16, 17, 18, 34, 74, 98, 99, 144, 204, 1-4, 1-5, 1-7	impacts	
degraded	22	operational	5, 88
degraded cyber	22	information assurance	vii, 8, 20, 24, 25, 29, 37, 203, 242, 1-3
socio-cultural	188	Information Assurance	4, 25, 55, 1-9
environments		Information Operations	26
adverse	5	information technology	vii, 1, 5, 9, 13, 55, 63, 64, 75, 98, 1-1, 2-2, 2-3, 3-6, 3-11
degraded	23	Information Warfare	<i>See</i> information operations
equilibrium	7, 20, 60, 61, 130, 201, 221, 1-6, 1-8	insurance	54
event management	6	integrity	vii, 2, 8, 20, 25, 29, 57, 99, 203, 208, 242, 1-2, 1-5, 1-9
exercises	22, 72, 180	Integrity	4, 130, 211
FAA	56, 8-9	interior	
FBI	24	soft	35
FCC	13, 14, 197	IRC	167, 170
Federal Communications Commission	13, 14	ISO	54, 2-12
feedback loops	21, 22	JOPES	112, 167, 168, 169, 170, 171
FFRDC	53	Joseph	
Finance	6, 1-2	Kenneth ‘Kenny’	v
FISMA	25	JWICS	108, 114, 115, 117, 168, 170, 171
forecast	vii, 1, 73, 130, 1-7, 1-8	Key Entities	44, 45, 95, 100, 109, 198
framework	9, 25, 55, 70, 110, 3-9, 4-10	Landwehr, Peter	v
organizational resilience	2, 21, 53, 54, 234	LDA	37, 38, 42, 43, 44, <i>See</i> LDA
risk management	6, 9, 10, 53, 55, 125	leaks	5
Gartner	14	learning	
Gligor, Virgil D.	v	experiential	62, 234
Goldwater-Nichols	85	organizational	21, 22, 41, 42, 63, 65, 75, 76
Google Scholar	37, 39, 2-1, 2-8	lessons learned	10, 32, 35
Graham, John	v	limiting factor	166
graph theory	2	Logistics	6, 1-2
heterogeneity	64	LSA	37, 38, 39, 40, 41
HR	6, 1-2	M&S	12, 13, 37, 38, 40, 57, 60, 71, 73, 74, 75, 76, 188, 247, 248, 250, 1-4
HRO	12, 17, 37, 56, 63, 188, 2-3	magnitude	19, 60, 61, 73, 134, 174, 178, 203, 3-12
HSPD	10, 17, 3-7	mal-adaptive	62, 132
HSPD-7	10	management	
hub nodes	173	cyber risk	37
Human Resource	6	disaster	37
Hurricane Katrina	10, 17, 32		
hybrid	57		
IA	26		
IBM	14		

Appendix 9 Index

risk	38	semantic	80
supply chain	58	networks	
MathJax	219	semantic	80, 81
matrix	41, 69, 131, 132, 189	New Jersey	32
measures of effectiveness	3, 19	New York	32
measures of interest	7, 132, 147, 165, 170, 172, 209, 244	Newtonian	62
measures of performance	3, 19, 73	ngram	81
MILDEC	27	NIST	25, 55
Military Deception	27	NMCI	54
mission assurance	vii, 1, 3, 6, 7, 9, 10, 28, 55, 77, 99, 102, 106, 126, 221, 238, 244, 249, 250, 1-2, 1-3, 1-4, 2-2	nonrepudiation	4, 8, 21, 1-9
mitigation	1, 2, 10, 27, 28, 53, 58, 76, 168, 170, 186, 209, 210, 213, 223, 227, 228, 230, 232, 236, 242, 250	nuance	3, 36, 172, 179
MITRE	53	OGA	113, 197
model	vii, 2, 4, 5, 10, 25, 29, 35, 36, 53, 57, 58, 66, 69, 70, 71, 72, 74, 77, 78, 79, 81, 82, 85, 89, 90, 93, 95, 96, 98, 99, 100, 109, 110, 116, 119, 125, 126, 128, 132, 133, 143, 147, 148, 152, 153, 154, 156, 157, 158, 159, 161, 162, 164, 166, 173, 174, 175, 176, 177, 181, 182, 183, 184, 185, 187, 188, 191, 193, 197, 198, 204, 205, 208, 209, 211, 215, 237, 240, 241, 242, 249, 1-1, 3-1, 3-5, 3-7, 3-12	Okasaki, Dr. Chris	v
final	96	ontology	4, 8, 106, 126, 191, 192, 220, 240, 242, 243, 244, 245, 1-5, 3-8, 3-9
M&M	35	operations	
mental	81	effects based	21
meta	96	military	6, 87, 110, 198, 1-2
modifications	2, 22, 77, 92, 125, 126, 138, 139, 140, 141, 192, 193, 250, 4-1	OPORD	205
MoI	129, 130, 143, 144, 148, 151, 154, 157, 158, 159, 161, 162, 171, 173, 174, 175, 176, 177, 180, 182, 209, 1-6, 1-7	optimality	57
Morgan		ORA	37, 39, 41, 44, 45, 46, 73, 95, 100, 119, 133, 135, 136, 137, 144, 147, 164, 165, 167, 169, 175, 191, 208, 214, 218, 220, 2-1, 2-3, 2-4, 2-10, 2-11, 3-6, 5-15, 6, 12, 14, 15
Geoffrey P.	v	orders	
multimodal	2	cyber related	88
multiplex	2, 70, 77, 78, 126	organization	vii, 1, 2, 3, 4, 5, 10, 12, 18, 27, 28, 42, 52, 53, 55, 58, 59, 60, 61, 63, 72, 73, 74, 75, 76, 77, 78, 79, 81, 82, 84, 88, 95, 100, 103, 106, 113, 119, 125, 128, 130, 131, 132, 135, 137, 139, 141, 143, 144, 145, 147, 148, 151, 156, 159, 161, 164, 166, 167, 170, 175, 181, 191, 198, 203, 206, 209, 210, 229, 235, 240, 241, 1-2, 1-4, 1-6, 1-7, 1-8, 2-2, 2-3, 3-9, 3-10
network		high reliability	12
co-citation	50	high reliability	12
meta	67, 68, 69, 70, 77, 81, 82, 92, 101, 106, 119, 126, 132, 133, 145, 159, 177, 179, 183, 191, 192, 240, 2-3, 2-4, 2-5, 2-6, 2-7, 2-11, 3-9, 3-12	self	56
		perception	10, 17, 21, 22, 23, 27, 35, 46, 88, 126, 144, 190, 242, 245, 250, 2-2, 17, 22
		organizational	22
		performance as accuracy	70, 160, 180, 181, 182, 226, 227, 8-10

Appendix 9 Index

Perl	83	Sandy	
perturbations	20, 62, 72, 1-8	Super Storm	10
Pfeffer, Jürgen	v	SCADA	11, 18, 32
power-law	173	Schneier	
probability of occurrence	28, 52	Bruce	30
Protection Analysis Project	28	SCM	12, 56, 57, 58, 70, 8-10
proxies	62, 65	SECDEF	109, 110
random outages	165, 173	security level	5
RBV	63	SEI	53, 55
recovery		self-perceptions	22, 161
post-event	6	semantic network	75, 80
reduction 27, 52, 53, 73, 137, 224, 2-8, 4-3		single point of failure	<i>See</i> SPOF
risk	52	SMART	70
regular expression	83	SNA	2
rehearsal	9, 24	snapshots in time	1, 10
pre-event	6	social network analysis	2, 44, 128, 144, 183
rehearsals	23, 54, 210, 230, 237, 1-8	soft interior	35
repetition	22	SPOF	134, 8-10
resilience	1, 7, 12, 19, 21, 28, 37, 41, 42, 57, 59, 60, 61, 62, 65, 72, 73, 105, 115, 116, 128, 129, 130, 131, 132, 133, 134, 139, 142, 143, 144, 145, 147, 148, 154, 159, 164, 184, 185, 188, 204, 209, 210, 230, 243, 249, 250, 1-2, 1-3, 1-4, 1-5, 1-6, 1-7, 1-8, 2-2, 2-3, 3-12, 4-7	stochastic	7, 38, 57, 189, 218, 220
organizational	1, 8, 12, 13, 17, 21, 42, 72, 74, 75, 77, 126, 132, 181, 249, 250, 1-4, 2-2, 2-3	Storm	
resiliency	vii, 157, 185, 4-2	Sandyjjjjjjj	32
resilient	1, 20, 27, 34, 36, 59, 60, 61, 63, 64, 76, 95, 141, 164, 173, 235, 1-3, 1-4, 2-2	structure	
retention		organizational	56, 63, 64
risk		Sun Tzu	29
RINSE	70, 72, 188, 8-10	Super Storm Sandy	10, 17, 32
risk		supervisory control and data acquisition	<i>See</i> SCADA
reduction	6, 55	supply chain	11, 12, 18, 36, 41, 57, 58, 70, 75
residual	20, 53, 54	management	58
risk assessment	2, 58	Supply Chain Management	<i>See</i> SCM
risk avoidance	52	SymSuite	70
risk management	6, 7, 9, 10, 13, 24, 27, 28, 37, 39, 41, 42, 52, 53, 54, 55, 58, 65, 75, 125, 126, 183, 238, 250, 1-9	SYN flood	25
cyber	27	text mining	vii, 2-3
cyber	27	theory	
RISOS	28	semantic network	80
		thesaurus	83, 3-1
		acronym	83
		case sensitive	83
		CASOS	93
		dissertation	83, 93
		final	98
		master	98
		model-specific	83
		Thesaurus	93, 2-8, 2-12

Appendix 9 Index

threats			
cyber	10, 17, 29	vulnerabilities	
transfer		structural	vii, 1, 182
risk	27, 28, 52, 54, 151, 4-13	Watson, Tom	14
unambiguous	63	Wei, Wei	v
USAF	6, 23, 87, 88, 95, 103, 197, 1-2, 1-3	wget	3-1
USG	24, 29, 31, 54, 72, 83, 99, 114, 3-1	White House	16
USMA	v	Wizard	
vectors		D2M	81, 85
attack	5	work product	83